الجرائم المستحدثة

المعلوماتية . الإلكترونية . السيبرانية

د. عماد مفلح الحسبان   د. عز الدين أحمد النعيمي

د. عدنان محمد الضمور   د. ياسر طالب الخزاعلة





الجرائم المستحدثة

(المعلوماتية - الإلكترونية - السيبرانية)

الجرائم المستحدثة

(المعلوماتية – الإلكترونية – السيبرانية)

الطبعة الأولى

2024



الجرائم

المستحدثة

(المعلوماتية - الإلكترونية - السيبرانية)

د. عماد مفلح الحسبان

د. عدنان محمد الضمور

د. عز الدين أحمد النعيمي

د. ياسر طالب الخزاعلة





رقم الإيداع لدى دائرة المكتبة الوطنية

(1351 /2024/3)

عنوان الكتاب: الجرائم المستحدثة : المعلوماتية، الإلكترونية، السيبرانية

تأليـــــــــــف: الحسبان، عماد مفلح سليمان

تأليف (آخرون):الضمور، عدنان محمد اسعيد

النعيمي، عزالدين أحمد شتيوي

الخزاعلة، ياسر طالب راجي

بيانات النشـــر: دار الخليج للنشر والتوزيع، 2023

الوصف المادي: 220 صفحة

رقم التصنيـــف: 364.168

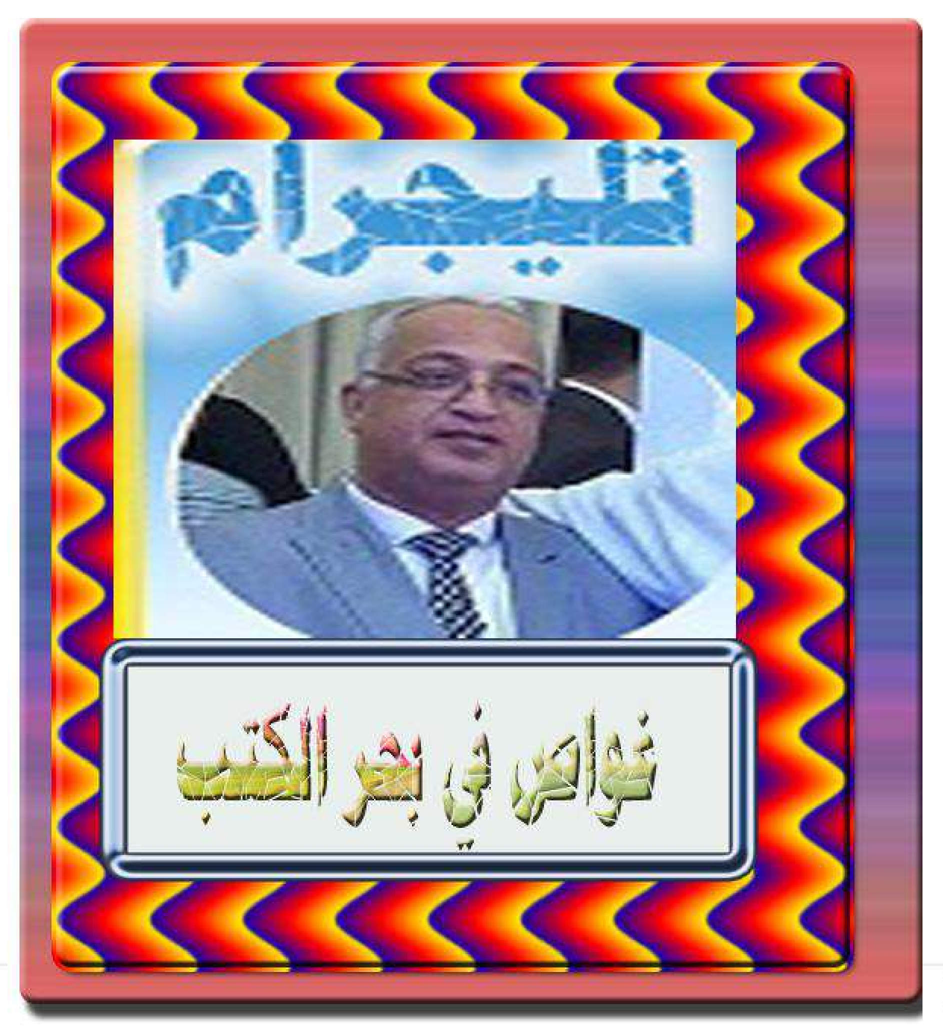
الواصفـــــــــات: /الجـرائم الحاسـوبية//أمـن الحاسـوب//شـبكات المعلومات//الجرائم ضد الملكية/

الطبعــــــــــــــة: الأولى

- يتحمل المؤلف كامل المسؤولية القانونية عن محتوى مصنفه ولا يعـبر عـن رأي دائرة المكتبة الوطنية أو أي جهة حكومية أخرى.

ISBN: 978-9923-23-198 -2

المحتويات


تليجرام
غواص في بحر الكتب

المقدمة

في أواخر تسعينيات القرن الماضي وأوائل القرن الحادي والعشرين، ومع بداية ظاهرة العولمة حدثت تغيرات كثيرة منها التقدم العلمي والصناعي والتكنولوجي، وظهور مفاهيم دولية جديدة في مجال العلاقات الدولية القائمة على تحرير التجارة العالمية والتحرر الاقتصادي، وتدويل الأنماط السلوكية الثقافية عالميا من خلال غزوالسلوكيات والثقافات الخاصة بالدول الأقوى اقتصاديا وعلميا وتكنولوجيا والتي تملك المفاتيح السحرية للتحكم في مجريات الأمور، من خلال سيطرتها على وسائل إبراز من فضائيات وخلافه؛ وأيضا التقنيات المستخدمة في كافة مناحي الحياة.

وأدى إلى إيجاد نمط متسارع من التقدم والنموفي بعض البلدان صاحبته آثار سلبية على الجانب الاقتصادي والاجتماعي والبيئي والأمني، مما أدى إلى إبراز أنماط مستجدة من الجرائم غير التقليدية؛ وظهور طوائف جديدة من التركيبات الإجرامية تختلف تماما عن تلك النمطية المعتادة سابقا. فعلى مستوى الجريمة ظهرت أنواع منها غير مألوفة لا تعتمد على استخدام الأساليب التقليدية؛ بل أصبحت تستعين بأحدث التقنيات ونتائج الدراسات العلمية والطبية والإلكترونية، ولا تركن إلى استخدام العنف في كافة جوانبها، بل أصبحت تعتمد على وسائل ذكية عبر أجهزة الحاسب الآلي التي صارت في متناول يد الجميع، وباتت أداة هامة تشكل درجة كبيرة من الخطورة في أيدي مرتكبي مثل هذه الصور من الجريمة. كما يتميز مرتكبوهذه الجرائم بالذكاء والثقافة العلمية والإلكترونية التي تساعدهم على اتقان وضع الخطط وآليات تنفيذها مع البراعة في إخفاء الأدلة لسرعة الإفلات من يد أجهزة

العدالة والشرطة. إذ ونحن على مشارف الالفية الثالثة يواجه العـالم ارتكـاب العديـد من الجرائم المستحدثة، وهذه الأخيرة انما هـي جـرائم تقليديـة لكنهـا ارتـدت ثوبـا جديدا باستخدام التقنيات المتقدمة، واصبحنا نواجه الان عولمة الجريمة والتي تشـكل في عصرنا الحديث تحديا وبات هذا التحدي اكثر عنادا وأشد استعصاء عـلى المكافحـة التقليدية حتى صار العمل الشرطي وكأنه عمل في حقل الألغام. (إبراهيم، 2001)

وعليه وفي ضوء المتغيرات الدولية والعلميـة والتقنيـة، بـدأت هـذه الطائفـة مـن الجرائم المستحدثة في الانتشار، وبصفة خاصـة في الولايـات المتحـدة الأمريكيـة ودول أوروبا الغربية في بادئ الأمر والتي انطلقت منها هذه المتغيرات، ووقعت فيها العديد من هذه الجرائم بصورها غير النمطية حيث كثفت الأجهـزة الشرطيـة مـن جهودهـا بهدف التعرف على هذه الجرائم ووضع خطط الوقاية والمكافحة لها وتعديل هياكلها التنظيمية لإنشاء وحدات أمنية قادرة على التعامل مع كل نمـط مـن أنماطهـا .إضـافة إلى اعداد الدراسـات والبحـوث الأمنيـة حـول أسـاليب ارتكابهـا وخصـائص مرتكبيهـا وصـفاتهم ودوافعهـم إلى ارتكابهـا وأوجـه الخـلاف بينهـا وبـين الجـرائم التقليديـة.(درويش، 1995)

وفي الآونة الأخيرة اتضح بـأن الجريمـة المسـتحدثة مازالـت لهـا اليـد الطـولى في السباق الدائر بينها وبين الأجهزة الشرطية، إذ لحقت بهـا مظـاهر التطـور المختلفـة سواء في الفكر(طريقة التخطيط لهـا) أو في الأداء (أسـلوب تنفيـذها) أو في الأدوات المستخدمة في ارتكابها. بل وإضافة إلى ذلك فقد جاء عصر العولمة وبمـا حملـه مـن ثورة في نظم المعلومات والاتصالات والانتقالات والتطور التكنولوجي؛ ليضيف أبعادا جديدة على مظاهر التطور الإجرامي الذي أدى إلى ظهـور أنمـاط مسـتجدة منهـا لم تكن مألوفة من قبل ؛ بل واشد خطورة على المجتمع من الجـرائم التقليديـة وهـذا

راجع لتسلحها بسلاح العلم والمعرفة والتقدم التقني ؛الأمر الذي أدى إلى حدوث أضرار جسيمة من جراء ارتكابها.(البدانية، 1998)

ضف إلى ذلك، فثورة تكنولوجيا الاتصالات والمعلومات، أوما يسمى الثورة المعلوماتية أوالرقمية، والتي واكبها تطور مطرد في مجال وسائل الاتصال وتقنياتها المختلفة، أحدثت زخما فكريا ومعنويا غير مسبوق. ولعل أبرز سمات هذه الثورة في مجال المعاملات قدرتها الفائقة على خلق فرص متنامية للمعاملات الإنسانية عن بعد، الأمر الذي اوجد في الواقع المنظور طائفة من المعاملات تتم عن طريق أجهزة الحاسب الآلي وتجرى وقائعها عبر شبكة الانترنيت. تلك الشبكة العملاقة التي بدأت مسيرة العمل كوسيلة اتصال وتبادل للمعلومات ثم أضحت بوابة المعرفة وفضاء اتصالي مفتوح على مصراعيه يزيل الحدود الجغرافية ويجعل من العالم اشبه بقرية الكترونية صغيرة.

كما أن الظروف الراهنة التي يمر بها العالم في إطار التنظيم الدولي الجديد وانتشار ظاهرة العولمة والذي تسعى فيه الدول الغنية والنامية على حد سواء إلى اللجوء للتكتلات الاقتصادية باعتبارها مدخلا أمنيا للألفية الثالثة كبديل عن التجمعات السياسية، إضافة إلى تزايد الصراعات الإقليمية والعرقية وضعف السلطات المركزية في العديد من مناطق العالم إلى جانب تعاظم عائدات الأنشطة غير المشروعة وبصفة خاصة المُستحدث والمُستجد منها، في ظل تعاظم وتنامي ظاهرة الفساد، وما أظهرته من أشكال جديدة ساهمت في وجود أنماط جديدة من الضغوط على الهيئات الحكومية وأجهزة الإدارة العامة في شتى أنحاء العالم كل هذا وغيره-أدى إلى توحش عصابات الإجرام المنظم وتزايد سطوتها ونفوذها وانتشار أنشطتها في مجال الجريمة وبصفة خاصة في مجال الجرائم المُستجدة أوالمستحدثة

منهـا، وهومـا يتطلـب تكـاثف أجهـزة الأمـن بكافـة مسـتوياتها الدوليـة والإقليميـة والوطنية لمواجهة هذا الخطر الداهم الذي يزداد انتشارا يوما بعد يوم.

يتنـاول هـذا الكتـاب أربعـة فصـول، حيـث استرسـل المؤلـف في الفصـل الأول بالتعريف في الجريمة والظواهر الإجراميـة وتطورهـا عـبر التـاريخ إلى أن وصـلت إلى الجرائم المعقدة، والتي تحتاج إلى تكنولوجيا عالية الدقة للتعامل معها والتصدي لها ومكافحتها، ويتنـاول الفصـل الثـاني أيضـا الجريمـة المعلوماتيـة والجريمـة الإلكترونيـة والمجرم الإلكتروني والخصائص والمميزات ومبدأ الأخطار والتنظيم التشريعـي للوثـائق الإلكترونيـة والإثبـات وإجراءاتـه ومعوقاتـه والتحليـل الجنـائي الرقمـي والمجـرم الإلكـتروني، وهنـا خـاض المؤلـف في تفاصـيل إثبـات الجـرائم المسـتحدثة وخاصـة الإلكترونية، وفي الفصل الثالث لخص المؤلف بالتفصيل الجريمة السيبرانية وعرف بها وشرح مفهومها، وركز على كل ما يتعلـق بهـا وبـالمجرم السـيبراني، وفي الفصـل الرابـع تطرق المؤلف إلى الجريمة الإلكترونية من منظور قانوني بحـت، وشرح أركـان الجريمـة الإلكترونية وعقوبتها واثارها الاجتماعية والأمنية والقانونية.

هذا الكتاب هوبمثابة مقدمة وبحث يمهد الطريق للباحثين في المستقبل للتوسع والإضافة في مجال الكتابة حول كل ما يتعلق بالجرائم المستحدثة، فمع مـرور الـزمن دائما تستحدث جرائم جديدة متنوعة تفرضها التغيرات والتطورات التـي تتجـدد كـل يوم، فهذا الكتاب يمثل نقطة انطلاق تبنى عليه الدراسـات المسـتقبلية حـول كـل مـا يستحدث من جرائم في المستقبل، نرجو من اللـه عز وجل أن نكون وفقنا في كتابتـه وأن يكون علما نافعا وصدقة جارية في ميزان حسناتنا واللـه من وراء القصد.

المؤلفين.

الفصل الأول

الجريمة والمجرم والظواهر الإجرامية

الفصل الأول

الجريمة والمجرم والظواهر الإجرامية

تمهيد

كانت الجريمة ولا تزال، تشكل مصدر قلق دائم ومتواصل، لكافة المجتمعات الإنسانية، وهي إحدى أخطر الظواهر التي تعمل على تدمير مقومات المجتمع، وتماسكه وقيمه، وتساعد على انتشار التفكك الاجتماعي، مما ينعكس على المجتمع بدخول ثقافة الإجرام المستهجنة، فيصبح الفرد فيه غير آمن على نفسه وماله، مما يجعله يشعر بالغربة في مجتمعه، فيضطر إلى تركه وهجره، أوإلى الانجراف وراء السلوك الإجرامي، ظنا منه أنه يحمي نفسه أوأنه يجد لنفسه مكانا بين أصحاب الثقافات المنحرفة والجرمية، لينال ثقتهم ويكون عنصرا فاعلا بينهم.

ويمثل ارتفاع معدلات الجريمة تحدياً كبيراً للمجتمعات، وخاصة أجهزة العدالة الجنائية التي تقع على مسؤوليتها الوقاية والمكافحة والمواجهة لكافة أشكال وأنماط الجرائم التي تعدت الأنماط التقليدية كالجرائم التي تقع على الأموال أوعلى الأشخاص، بل تحولت إلى جرائم ذات طابع تقني بعد دخول التكنولوجيا الحديثة في ارتكابها، مثل الجرائم الاقتصادية، والإرهاب، والمخدرات، وجرائم تقنية المعلومات. (**Brander**,2016)

ويعتبر عصرنا الحالي هوعصر انتشار الجريمة بلا شك فالجريمة حولنا في كل مكان والتخلص منها بشكل كامل حلم صعب المنال، وارتفاع معدلات الجريمة يمثل تحديا لأي مجتمع يريد أن يبقى ويزدهر لما تسببه من آثار مدمرة على الفرد

وعلى المجتمع، لذا يصبح خفض معدل الجريمة هدفا أساسيا لأي مجتمع من المجتمعات وذلك من خلال البحث في أسبابها وظهرت الجريمة في المجتمعات منذ القدم؛ إذ تعتبر الجريمة ظاهرة اجتماعية نشأت مع نشأة الحياة الاجتماعية على سطح الأرض، وقد احتلت الصدارة في العديد من الأبحاث والدراسات العلمية، وهذا بدروه أدى إلى ظهور الحاجة من أجل الكشف عن جوانبها وإخراجها إلى دائرة الفهم والتحليل.(الهراوة، 2015).

لقد شهدت المجتمعات البشرية تطوراً هائلاً في مختلف العلوم والمجالات، وخاصة في مجال التطور التقني والتكنولوجي، وأدى ذلك إلى المساهمة في استخدام هذه التقنيات للحد من الجريمة ومواجهتها، إلا أن العصابات الإجرامية، وكذلك الأفراد الذين لديهم النزعة الجرمية قاموا باستغلال تلك التقنيات لارتكاب الجرائم بواسطتها، فهي وسيلة فعالة لهم لتحقيق أهدافهم وزيادة مكتسباتهم، وبناء على ذلك تم تطوير الأساليب الجرمية، والتنويع في أنماط الجرائم، وطُرق ارتكابها، وكذلك تم التغيير في أنواع الضحايا المستهدفة بما يتناسب مع الأهداف والمكاسب المرجوتحقيقها.

المبحث الأول : الجريمة وماهيتها ومفهومها وتطورها وانواعها وتفسيراتها النظرية:

ماهية الجريمة وتطورها

الجريمة ظاهرة عرفتها البشرية منذ نشأتها وبداياتها الأولى، وقد دلنا القرآن الكريم على أول جريمة وقعت على الأرض، عندما قتل قابيل أخاه هابيل ظلما وحسدا، وذلك عندما تنازعته قوة الشر وقوة الحسد، ولم تمنحه فرصة التفكير أن فعله هذا سيزهق نفساً بشريةً قد صانها الله عزوجل وقدّسها، فجعل لقاتلها أشد العقوبات، حيث قال تعالى {وَاتْلُ عَلَيْهِمْ نَبَأَ ابْنَيْ آدَمَ بِالْحَقِّ إِذْ قَرَّبَا قُرْبَاناً فَتُقُبِّلَ مِن أَحَدِهِمَا وَلَمْ يُتَقَبَّلْ مِنَ الآخَرِ قَالَ لَأَقْتُلَنَّكَ قَالَ إِنَّمَا يَتَقَبَّلُ اللهُ مِنَ الْمُتَّقِينَ } (المائدة، آيه27).

وتعد الجريمة مشكلة اجتماعية خطيرة، ناتجة عن التفاعلات والعلاقات المترابطة بين الأفراد ذوي المصالح المتعارضة، وهي تشكل ظاهرة مرافقة للإنسان أينما وجد، ولهذا يتعذر منعها بصورة مطلقة، لكن بالإمكان تقليصها والحد منها نسبيا، وذلك بتجفيف منابعها ومعالجة العوامل المولدة لها، سواء أكانت بيولوجية، أم اجتماعية، أم اقتصادية، أم نفسية، أم ناتجة عن اختلالات أسرية وبيئية(الكساسبة، 2010).

مفهوم الجريمة في العلوم المختلفة

قبل البدء بالحديث عن الجريمة وتطورها، وما تناوله العلماء على مر العصور والأزمان في شأن الجريمة وأنواعها، وخصائصها، لابد من معرفة معنى الجريمة من جوانب متعددة منها: القانونية، والدينية، والاجتماعية، والمعنى العام للجريمة.

أولا: المفهوم العام للجريمة

الجريمة بمعناها العام ظاهرة اجتماعية وخُلقية وسياسية واقتصادية، قبل أن تكون حالة قانونية، وانطلاقا من هذا المفهوم يرى بعض الباحثين أنها عبارة عن تعبير للموازنة بين صراع القيم الاجتماعية والضغوط المختلفة من قبل المجتمع، فالإجرام هونتيجة لحالة الصراع بين الفرد والمجتمع، وقد كانت الجريمة في المجتمعات القديمة، تُعزى إلى نفس المجرم الشريرة، ولأن الانتقام هوالأساس في رد الفعل للسلوك الإجرامي (الجميلي، 2001).

الجريمة بالمفهوم القانوني:

ورد تعريف الجريمة بالمفهوم القانوني على أنها سلوك (فعل أوامتناع) غير مشروع، أخلّ بمصلحة أساسية، صادرة عن إرادة جنائية، يقرر لها القانون عقوبة، أوتدبير احترازي. (السعيد، 2006)

والجريمة من الناحية القانونية، هي كل فعل مخالف لأحكام قانون العقوبات، وهوالقانون الذي يتضمن الأفعال المُجرَّمة، ومقدار عقوبتها، وبما أن الجريمة هي فعل يضر بالمجتمع، فمن حق الهيئة الاجتماعية، أن تحافظ على سلامتها، بتشريع القوانين التي تتصدى لمن يعتدي على حرمتها، وتوضع العقوبات لتعاقب من يخالف أحكامها المُجرّمة (الجميلي، 2001).

الجريمة بالمفهوم الاجتماعي:

تُعد الجريمة في الأساس سلوكا مغايرا لقيم المجتمع ومعاييره السائدة، وهذه القيم والمعايير هي الضوابط التي تحدد سلوك الأفراد، وتمنعهم من الخروج عليها،

وذلك بسن القوانين التي تُجرم فعل هؤلاء الأفراد، وتفرض عليهم عقوبات اجتماعيـة، قد تصل إلى النفي، أوالعزل أوإلى الهجر في بعض المجتمعات.

وقد وردت مجموعة من التعريفات الاجتماعيـة للجريمـة لعـدد مـن البـاحثين في هذا المجال لدى (الجميلي، 2001) كما يلي:

يعرفهـا ثورســتن ســيلين (**Sellin,1968**) عــلى أنهــا ســلوك مخــالف للأعــراف الاجتماعية سواء كان هذا السلوك مخالفاً للقانون الجنائي أم لا.

أما دوركايم (**Durkheim**) فقد عرفها على أنها حقيقة اجتماعيـة وهـي ظـاهرة طبيعية للمجتمع، ولها وظيفتها الخاصة في خدمة المجتمع.

وعرفهـا بـراون (**Brown**) بأنهـا: خـرق للعـادات تثـير طلـب تطبيـق العقوبـات الجنائية.

الجريمة في علم الإجرام:

يقصد بالجريمة كظاهرة اجتماعية بأنها: كل فعل يتنـافى مـع القـيم السـائدة في المجتمع، وهي خطيئة اجتماعية تعارض قيم وأخلاق المجتمع(نجم، 2006).

ويعرفها جاروفالو (**Garovalo**) على أنها: فعل ضار في مختلف المجتمعات وكافة الأزمان، وأنها تتعارض مع مشاعر الشفقة ومشاعر الأمانـة أوالعدالـة، التـي تعارفـت عليهـا المجتمعـات الإنسـانية، وتتطـور بتطـور هـذه المجتمعـات عـلى مـر العصـور، وتتوارثها الأجيال جيلا بعد جيل (الوريكات، 2009).

تطور الجريمة وتفسيراتها النظرية:

الجريمة موجودة منذ القدم، فهي ظاهرة موجودة قبـل خلـق الـبشر حيـث دلنـا القرآن الكريم على معصية إبليس لـرب العـالمين عنـدما أمـره بالسـجود لآدم فـرفض،

ولذلك أوقع الـلـه عزوجل عليه العقوبة وهي الخـروج مـن الجنـة، واللعنـة إلى يـوم القيامة ثم يكون مصيره نار جهنم خالداً فيها، ثم أشار القرآن إلى عدة حالات تم فيها ارتكاب الجرائم وهذا حسب التعريف القـانوني الـذي تـم الإشـارة إليـه، ومـن هـذه الحالات عندما خاطب الـلـه عزوجل الملائكة بأنه سيجعل في الأرض خليفة، فكـان رد الملائكة على رب العزة بأنه كيف سيكون في الأرض بشر وقد كان لهم تجربة مع مـن سبقه من الخلق في القتل وسفك الدماء، والفساد فيها، ثم جـاءت معصـية آدم عليـه السلام عندما أكل من الشجرة التي نهاه الـلـه عـن الأكـل منهـا، فكانـت العقوبـة أن ينزل من الجنة إلى الأرض، ومنهـا بـدأت الحيـاة البشريـة فـتم ارتكـاب الجـرائم مـن قبلهم، حيث كانت أول تلك الجرائم هـي قتـل هابيـل عـلى يـد أخيـه قابيـل بـدافع الحسد والغيرة، وبذلك ارتبط وجود الجريمة على الأرض بـالوجود الإنسـاني، وبـدوافع الخير والشر، وبالفطرة الإنسانية..

وفي المجتمعات البدائية شهدت أنواعاً مختلفة من الجـرائم، حيـث لا تـزال تلـك الجرائم مستمرة إلى وقتنا الحاضر في أنماطها المختلفة متمثلة في أنواع عديدة؛ منها ما يقع على الإنسان وسلامته الجسـدية وحقـه في الحيـاة، ومنهـا مـا يقـع عـلى الأمـوال والممتلكات، وغيرها من الأنماط المختلفة إلى أن ظهرت الجرائم الحديثة التي تطـورت أساليبها بتطور الوسائل والتقنيات الحديثة التي ساهمت في ارتكاب تلك الجرائم.

لقد كانت الجريمـة تـفسر بتفسـيرات تفتقـر في الغالـب إلى الطـابع العلمـي، ولم تسـتند تلـك التفسـيرات إلى الأسـس المنطقيـة، فظهـر التفسـير الفلسـفي أوالـديني للجريمة، إذ سـاد الاعتقـاد قـديما بـان أرواحـاً شريـرة تـتقمص أجسـاد بعـض الأفـراد وتدفعهم إلى ارتكاب المحرمات (عبد المنعم، 2003).

ولأن هذه التفسيرات كانت محدودة الفهم، وانحصرت العوامل المؤدية إلى الجريمة حسب معتقداتهم بوجود تلك الأرواح الشريرة، فكان من الطبيعي أن يتم اللجوء إلى ضرب الشخص المُرتكب للجريمة، وتعذيبه من أجل تخليصه من تلك الأرواح الشريرة كما يعتقدون (الشاذلي، 2006).

أما عند اليونان فالجريمة تعتبر شاذة في المجتمع الإنساني، فقام فلاسفة الإغريق بدراسة الجريمة، والوقوف على أهم العوامل المؤدية لها، فقد اهتم أرسطو(384-322) قبل الميلاد، بالعلاقة بين الجريمة والسمات الجسمانية للفرد، مثل ملامح الوجه، شكل الجبهة، كثافة الشعر، لون البشرة، كما ربط بين الجريمة والفقر، ويرى أن الفقر يولد الميل إلى الرذيلة، والجريمة إحدى صورها (الوريكات، 2010).

وعند ظهور علم الجريمة كعلم مستقل في دراسة الجريمة، تغيرت النظرة إلى التفسيرات الغيبية أوالفلسفية، بل أصبحت تلك التفسيرات تعتمد على الدليل العلمي، والبحث في العوامل المؤدية إلى ارتكاب تلك الجرائم ودراستها من كافة النواحي بأسلوب علمي قائم على التجربة والملاحظة والاختبار، وكذلك دراسة شخصية المجرم والضحية دراسة شاملة للوقوف على الدوافع الفردية والمجتمعية التي تقف وراء ارتكاب تلك الجرائم، من أجل الوقاية منها والحد من انتشارها.

أما الجريمة في الشريعة الإسلامية تعرف على أنها: محظورات شرعية زجر الله تعالى عنها بحد أوتعزير، وهذه المحظورات قد تكون، إتيان فعل منهي عنه، أوترك فعل مأمور به، وتعد هذه الأفعال جرائم، لأنها تشكل ضررا بنظام الجماعة، أوبأفرادها، أوبأموالهم وممتلكاتهم، وأعراضهم، وغير ذلك مما يستوجب معه صيانة حال الجماعة (الوريكات، 2009).

وتنقسم الجرائم في الشريعة الإسلامية وفقاً لجسامة ما يتقرر لها من عقوبات في التشريع الجنائي الإسلامي إلى الاقسام الآتية: (عوده، 1998)

جرائم الحدود: وهي الجرائم المعاقب عليها بالعقوبة المقدرة حقاً لله تعالى، أي أنها محددة معينه، ليس لها حد أدنى ولا حد أعلى، كما أنها لا تقبل الإسقاط لا من الجماعة ولا من الأفراد مثل: جرائم الزنا، القذف، شرب الخمر، السرقة، الحرابة (قطع الطريق)، الردة، البغي.

جرائم القصاص والدية: وهي الجرائم التي تقع على النفس كالقتل العمد، أوالقتل الخطأ، أوتقع ما دون النفس، كالجرح والإيذاء، والعقوبات المقررة على تلك الجرائم هي عقوبات مُقدّرة للأفراد وللمجني عليه أن يعفوإذا شاء وبذلك تسقط العقوبة عن الجاني.

جرائم التعزير: وهي العقوبات على الذنوب التي لم تقرر لها الشريعة الإسلامية عقوبة مُقدّرة، وتبدأ بالعقوبات البسيطة وتنتهي بأشد العقوبات كالحبس والجلد والقتل في الجرائم الخطيرة، ويتمتع القاضي بسلطة تقديرية في تحديد عقوبات هذه الجرائم بما يتناسب مع حال المجرم ونفسيته وسوابقه.

أنواع الجرائم

تنقسم الجرائم إلى عدة أنواع منها:

- الخطورة الجرمية

تُقسم الجرائم من حيث خطورتها إلى عدة أقسام يعتمد التصنيف الأول فها على أساس العقوبة، فقد تم تقسيم الجرائم إلى الأقسام التالية:

الجناية: وهي الجرائم ذات العقوبات العالية بحسب درجة خطورة الفعل الإجرامي، وهذه العقوبات تشمل الإعدام، والأشغال الشاقة المؤبدة، والأشغال الشاقة المؤقتة، والسجن لفترات طويلة حددها القانون، ولعل الجانب المهم في تصنيف الجرائم بمقتضى الركن القانوني تأخذ أهمية أكبر من الجرائم التي يتم تصنيفها بحسب الركن المادي أوالمعنوي، حيث يعتمد القانون الأخذ بالعقوبات المقررة لكل جريمة. (أبوعامر، 1993)

الجنحة: وهي الجرائم التي يتم معاقبة مرتكبيها بالحبس أودفع الغرامة المالية، وتعتمد مدة العقوبة على ظروف ارتكاب هذه الجرائم (ظروف مخففة أومشددة) حيث يأخذ القاضي بها عند إصدار الحُكم على الجاني. (أبوعامر، 1993)

المخالفة: وهي الأفعال التي يقوم بها الشخص أويمتنع عن القيام بها ويترتب على ذلك عقوبة قانونية، وهي تتراوح في الغالب بين الحبس لمدة لا تزيد عن شهرين، أوالغرامة المالية حسب ما ينص عليه القانون. (روابح، 2019)

وهنا يمكن التمييز بين هذه التقسيمات على أساس مقدرا العقوبة فعقوبة الجناية مختلفة عن الجُنح والمخالفات، وأن معيار التمييز بين الجُنحة والمخالفة هوالعقوبة التي نص عليها القانون، ويكون مقياس العقوبة في حدها الأقصى دون الحد الأدنى.(السراج، 2018)

ومن أهم النتائج التي تترتب على تقسيم الجرائم بهذه الطريقة تكمن في الأحكام التي تخضع لها الجرائم، سواء من الناحية الإجرائية، أومن الناحية الموضوعية، فمن الناحية الإجرائية فقد حدد القانون الإجرائي أن محاكم الجنايات هي التي تنظر في القضايا الجنائية وبعض الجُنح التي تقع ضمن اختصاصها استثناءً من الأصل العام، فالتحقيق الابتدائي هوشرط أساسي لصحة المحاكمة خاصة في الجنايات، أما الجُنح

والمخالفات فهوأمر جوازي للمحقق، كما يعتبر الحبس الاحتياطي هوأمر جائز في الجنايات عموماً، ويجوز في الجُنح في بعض حالات التي حددها القانون، بحسب مدة الحبس التي لا تزيد عن ثلاثة أشهر، أما في المخالفات فلا يجوز الحبس الاحتياطي إطلاقاً، كما يمكن التمييز بين هذه التقسيمات بحسب مدة التقادم للدعوى والعقوبة فهومختلف بحسب ما إذا كانت الجريمة جناية أوجُنحة أومخالفة(أبوعامر، 1993)

- القانون الموضوعيّ:

إنّ السريان الشخصي لأحكام القانون الموضوعي، يكون على ما يرتكبه الشخص من جرائم خارج بلده الأم، فإذا ما عاد فإنه يلزم به، من بين ما يلزم من شروط، على أن تكون الجريمة المنسوبة إليه ارتكابها جناية أوجنحة معاقب قانونًا، فالقانون لا يُعاقب على الشروع في المخالفات، ولا على الشروع في الجُنح إلا في حدود معينة وهي محددة بنص خاص، أما في الجنايات فيعاقب على الشروع إلا إذا وجد نص يقرر خلاف ذلك، أما الاتفاق الجنائي فيتم العقاب عليه إذا كان القصد منه ارتكاب جناية أوجنحة.

إن مصادرة الأشياء المتحصلة من جريمة أوالمستعملة فيها لا تكون إلا إذا كانت الجريمة المرتكبة جناية أوجنحة.

وعلى هذا الأساس فإن العبرة في التقسيم الثلاثي للجرائم من جسامة وخطورة الفعل المرتكب، يكمن بالعقوبة التي يقررها نص القانون، لا بالعقوبة التي ينطق بها القاضي، فالقانون على سبيل المثال يقرر لجريمة السرقة البسيطة عقوبة الحبس الذي

لا يزيد أقصى مدة له عن سنتين، وهذا يعني أنها (جنحة)، وسوف يظل هذا الوصف قائمًا، حتى لوحكم القاضي بأقل من العقوبة المقررة لهذه الجريمة.

- **طبيعة الجريمة المرتكبة:**

حاول الفقه الجنائي التمييز بين الجرائم بحسب طبيعتها، وذلك من خلال معياري طبيعة الجريمة وطبيعة الفئة المستهدفة من هذه الجرائم، ومن أن التقسيمات للجرائم بحسب طبيعتها هي ما يلي: (السراج، 2018)

الجرائم السياسية: هي الجرائم التي تهدف إلى إزاحة من يمتلكون زمام الحُكم، وهذا النوع من الجرائم قديم جداً قِدَم السلطة نفسها، ويُسمى من يقوم بهذه الجرائم بالمعارضين، ولذلك قد تصل عقوبة هؤلاء إلى حد القتل.

فهذه الجرائم يتم الاعتداء فيها على النظام القائم في الدولة، وعلى دستورها، ولذلك يُصنف الفقه الجنائي الجرائم السياسية وفقاً لمعيارين: الأول هوالمعيار الشخصي؛ وهوالمعيار الذي يعتبر الفعل المرتكب جريمة سياسية إذا كان الباعث على ارتكابها هوباعث سياسي، مثل قلب النظام السياسي الحاكم في الدولة. أما المعيار الثاني فهوالمعيار الموضوعي الذي يتم اعتبار الفعل بموجبه جريمة سياسية، عندما يكون الهدف منه المساس بالحقوق السياسية لمؤسسات الحُكم أوالمساس بحقوق المواطنين السياسية. (السراج، 2018)

الجرائم الاجتماعية: وهي الجرائم التي تقع ضد القيم والقواعد العامة في المجتمع، وتهدف هذه الجرائم إلى إلحاق الأذى والضرر بالمصالح الاجتماعية في المجتمع، وتتنوع أسباب تلك الجرائم منها ما هومتعلق بالفرد وسلوكه الإجرامي، ومنها ما هومتعلق بالتنشئة الأسرية والاجتماعية، ومنها ما هوبيئي يتعلق بمكان

السكن أوالعمل، ويأتي على رأس تلك العوامل ضعف الوازع الديني لدى الأفراد مرتكبوهذه الجرائم، ومن هذه الجرائم ما يلي: (بوالماين، 2008)

جرائم ضد ممتلكات الأفراد؛ مثل اضرام الحرائق المتعمدة بأملاك الآخرين وتخريبها، الإيذاء الجسدي، القتل، جرائم ضد النظام العام مثل جرائم إشاعة الفوضى والتخريب.

الجرائم الدينية: مثل الاعتداء على دور العبادة وتخريب ممتلكاتها والاخلال بالنظام فيها جرائم ضد الأسرة كالخيانة والإهمال والزنا.

جرائم ضد الأخلاق: مثل الأفعال الفاضحة والجارحة للحياء في المناطق العامة.

جرائم ضد المصادر الحيوية للمجتمع: مثل تبديد ثروات المجتمع، الصيد في غير موسمه وغيرها.

الجرائم الاقتصادية: هي عبارة عن القيام بفعل أوالامتناع عن الفعل الذي حدده القانون بأنه مخالف للقواعد التي تسعى لحماية السياسة الاقتصادية للدولة، أوحماية الاقتصاد القومي، وهذه الأفعال تلحق الضرر بعمليات الإنتاج للسلع والخدمات وتوزيعها واستهلاكها، ومن صور تلك الجرائم: (عمراني، 2014)

- **جرائم الاخلال بتنفيذ الالتزامات الاقتصادية**

جرائم الاستفادة بغير حق على حساب الاقتصاد العام.

الجرائم العسكرية: هي الجرائم التي ترتكبها الأشخاص الذين يحملون الصفة العسكرية أوأن يكون المجني عليه يحمل الصفة العسكرية، أوأن يكون محل الجريمة يحمل الصفة العسكرية مثل؛ المباني، المستودعات، معدات الأسلحة، السيارات والآليات، وغيرها، وهي سلوك يتم الاعتداء به على المصالح العسكرية في الدولة، وهذه

المصالح تحميها القوانين والأنظمة العسكرية، بموجب أوامر وتعليمات توجه إلى العاملين في القوات المسلحة، وتنقسم الجرائم العسكرية إلى قسمين:

الجرائم العسكرية البسيطة: ويتم تجريمها من قبل قانون الاحكام العسكرية.

الجرائم العسكرية المختلطة: وهي الجرائم أوالأفعال التي يجرمها قانون العقوبات، وقانون الأحكام العسكرية.

الجرائم الإرهابية: وهي الجرائم التي يتم الاعتداء فيها على الأشخاص أوالممتلكات أوكلاهما، ويكون القصد من ارتكاب الفعل هوتخويف الناس وبث الرعب في نفوسهم، ونشر الفوضى في المجتمع، والتأثير على الحياة في المجتمع. (أقبلي والعمراني، 2020)

وللجرائم الإرهابية أركان كغيرها من الجرائم تتمثل في الركن القانوني أوالشرعي، وهووجود النص القانوني الصريح الذي يُجرم هذا الفعل أوالامتناع عنه، 13 أما الركن المادي في الجرائم الإرهابية فيتمثل في النشاط المادي من المجرم الإرهابي، سواء كان هذا النشاط عمل أوامتناع عن العمل. (أقبلي والعمراني، 2020)

أما الركن المعنوي: فهوقيام المجرم الإرهابي بتوجه نشاطه من أجل تحقيق فعل مُجرّم وهذا الفعل مصنف ضمن الجرائم الإرهابية. (أقبلي والعمراني، 2020)

جرائم الحق العام: وهي الجرائم التي تستهدف الاعتداء الأشخاص، وعلى الممتلكات العامة والخاصة، ويقصد الجاني من ارتكابها تحقيق منفعة شخصية له، دون استهداف بث الرعب والخوف في نفوس الناس. (القصير، 2006)

- **صورة الفعل:**

حيث قسم القانون الجنائي الجرائم بناء على صورة الفعل إلى عدة أقسام كما يلي:

جرائم ضد الأشخاص: وهي الجرائم التي تستهدف الأشخاص سواء الاعتداء أوبالتهديد، أوالتي تمس حق أساسي من حقوق الشخص المعتدى عليه، ويدخل ضمن هذه الجرائم جميع الأفعال التي تستهدف الاعتداء على الشرف والعِرض، وتُصنف الجرائم ضد الأشخاص بأنها من أخطر أنواع الجرائم، فهي تهدد الكيان البشري وسلامة الانسان، وقد ميز الفقه الجنائي بين عدة أنواع من الجرائم ضد الأشخاص منها؛ الجرائم التي تمس حقوق الإنسان الأساسية مثل؛ القتل العمد، القتل الخطأ، والنوع الآخر هوالجرائم التي تمس حقوق الإنسان الثانوية مثل؛ جرائم التعذيب والاختفاء القسري.

ومن أبرز هذا النوع من الجرائم في الأردن هي: الشروع بالقتل، القتل مع سبق الإصرار(العمد)، القتل القصد، الضرب المفضي إلى الموت، القتل غير القصد (القتل الخطأ)، الإيذاء البليغ.

جرائم ضد الملكية: وهي الجرائم التي تستهدف الحقوق ذات الطابع الاقتصادي أوالمالي، التي يتم فيها الاعتداء أوالحاق الضرر بحق له قيم مالية ويدخل في نطاق التعاملات الاقتصادية مثل النصب وخيانة الأمانة والسرقة. (أقبلي والعمراني، 2020)

ومن صور هذه الجرائم في الأردن هي: السرقة الجنائية، السرقة الجنحوية، الشروع بالسرقة، الاحتيال، سرقة السيارات.

جرائم ضد الآداب: وهي الجرائم التي تُشكل خرق واضح للآداب العامة في المجتمع؛ مثل جرائم الاغتصاب، والخيانة الزوجية، وجرائم هتك العرض، والدعارة وغيرها، وعليه يمكن اعتبار كل جرائم العرض تتمثل في الممارسات

الجنسية التي تكون خارج إطار العلاقة الزوجية المشروعة، سواء كانت برضا الطرفين أوبالإكراه.

ومن أهم صور جرائم العرض ما يلي:

1. نشر الرسوم أوالصور المنافية للآداب العامة.
2. الاخلال العلني بالحياء.
3. التحريض على ممارسة الرذيلة.
4. جرائم الانتهاك أوالاخلال بالآداب العامة.

ومن أبرز هذا النوع من الجرائم في الأردن هي: الاغتصاب، الخطف، هتك العرض، جرائم البغاء، الزنا، الإجهاض.

- **جرائم بحسب الدافع الإجرامي**

صنف علماء الجريمة الجرائم بحسب الدافع الجرمي إلى عدة أنواع، ويمكن توضيح هذا النوع من الجرائم بما يلي: (البشري، 2007)

جرائم العنف: وهي الجرائم التي تكون كرد فعل على العنف المضاد أوأي تصرف يكون فيه هجوم، أوعلى أي عمل يظن المجرم أنه هجوم ضده، مثل جرائم القتل، والإيذاء، والضرب، والجروح، والكسور.

الجرائم النفعية: فتضم مجموعة الجرائم التي يستهدف الهجوم من ورائها تحقيق نفع ذاتي أوأناني محض كالحصول على حريته الشخصية، مثل التخلص من شخص يشكل قيداً على حرية هذا الشخص، أوالتخلص من ممتلكات أوأموال مؤمن عليها من أجل الحصول على قيمة التأمين.

جرائم إرساء العدالة الكاذبة: وهـي أسـاليب يسـتخدمها المجرمـون كأسـاليب رد فعل على نظام العدالة الجنائية، الذي يعتـبره هـؤلاء بأنـه غـير منصـف لهـم، لـذلك يلجأون إلى الجريمة ظناً مـنهم أنهـم يقيمـون الحـق، ويغلـب عـلى جـرائمهم الطـابع العاطفي مثل الحماس الزائد، الغيرة، الحب، الكراهية، وأحياناً تكون بدافع ديني قائم على المذهبية أوالطائفية، أوالتطرف فيحـاول أن يسـتخدم القـوة مـن أجـل الانتصـار لمذهبة أوفكره.

جرائم الشفقة أوالاشفاق: وهي الجرائم التي ترتكب بـدافع الشـفقة مثـل؛ قتـل المـريض الـذي لا يعـاني مـن أمـراض مزمنـة وخطـيرة ولا يتوقـع شـفاؤه مثـل قطـع الأوكسجين عنه، أوقتل طفل ولـد مشـوهاً فهـذا الفعـل يعـده الـبعض جـائزاً بـدافع الشفقة على الشخص وتخليصه من الآلام، ومنهم من يُطلق على هذا النوع من القتل بالقتل أوالموت الرحيم.

جرائم بلا ضحايا: وهي الجرائم التي تؤدي إلى الخسائر التـي اسـتعملت كنتيجـة للنشاط الجرمي، وكذلك انفاق بعض موارد الدولة سـنوياً في مكافحـة هـذه الجـرائم وملاحقة مرتكبيها في حال وقوعها.

الخصائص العامة للجريمة:

تتميز الجريمة بمجموعة من الخصائص التي يجب توافرها للحُكم على الفعل بأنه يُشكل جريمة، ومن هذه الخصائص ما يلي: (طالب، 2001)

- الضرر وهوالمظهر الخارجي للسـلوك، فالسـلوك الجرمـي يـؤدي إلى الحـاق الضرر بالمصالح الفردية أوالاجتماعية أوكلاهما، وهذا هوالركن المادي للجريمة فلا يكفـي القصد اوالنية وحدهما.

- التجريم القانوني: يجب ان يكون هـذا السـلوك الضـار محرمـا قانونيـا ومنصوصـا عليه في قانون العقوبات.

- ضرورة وجود تصرف سواء كان ايجابياً أوسلبياً، عمـديا ام غـير عمـدي يـؤدي إلى وقوع الضرر، ويقصد من هذا القول توافر عنصر الحرية واختفاء عنصر الاكراه.

- توافر القصد الجنائي فالجريمـة التـي يرتكبهـا الانسـان العاقـل عـن قصـد ورغبـه وتصـميم تختلـف عـن تلـك التـي يكـره الانسـان عليهـا اوالتـي يرتكبهـا الطفـل اوالمجنون.

- وجود توافق بين التصرف والقصد الجنائي ومثالا على ذلك ان رجل الشرطة يدخل منزلا ليقبض على شخص ما بأمر من القاضي اوالمسئول ثـم يرتكـب جريمـة اثنـاء وجوده في المنزل بعد تنفيذ امر القبض لا توجه اليه تهمـه دخـول المنـزل بقصـد ارتكاب جريمة لان القصد الجنائي والتصرف فيها لم يتلاقيا معا.

- توفر العلاقة بين الفعل المُحرم قانوناً وسوء التصرف اوالسلوك حتى يمكن تجريمه.

- توفر مبدأ الشرعية ويعني وجود عقوبة منصوص عليها قانونـاً للفعـل المجُـرّم، إذ تنص القاعدة القانونية أنه لا جريمة ولا عقوبة إلا بنص.

المبحث الثاني: مفهوم المجرم وانواع المجرمين وانماط المجرمين وتصنيفاتهم

المجرم

تعتبر دراسة المجرم وهوالشخص الذي قام بارتكاب الفعل المرحلة التالية في دراسة الظاهرة الجرمية، إذ أن المجرم هوأحد الأركان الأساسية في العملية الجرمية، حيث لا يوجد فعل بدون فاعل، لذلك لا بُد من دراسة الفاعل دراسة شاملة من جميع الجوانب الخاصة به وبمحيطة الاجتماعي حتى نستطيع فهم شخصيته وفهم الأنماط الجرمية التي يقوم بارتكابها.

المفهوم القانوني للمجرم:

المجرم هوالشخص الذي يرتكب فعل من الأفعال التي جرمها القانون سواء كان هذا الفعل ايجابيا أم سلبيا، وصدر بحقه حُكم قضائي نهائي بإدانته (القهوجي، 2002، ص21).

ويتبين من خلال هذا التعريف أنه لا بد من توافر شرطين لكي يُعد الشخص مجرما من الناحية القانونية هما (الوريكات، 2009، ص56):

أن يرتكب الشخص محل البحث واقعة أوفعلاً (سلبي أوايجابي) يُعد جريمة وفقا لنص التجريم القانوني ووفق مبدأ شرعية العقوبة إذ لا جريمة ولا عقوبة إلا بنص قانوني، مع إرادته لهذا الفعل وعلمه بما يترتب عليه من نتائج.

ثبوت إدانته أمام المحكمة أمام المحكمة بارتكاب الجريمة، فلا يكفي لاعتبار الشخص مجرما في نظر القانون أن يرتكب فعلا مجرما وفقا لنص التجريم، بل لا بد أن يدان أمام القضاء بارتكاب هذه الجريمة بحكم قضائي قطعي، تطبيقا للقاعدة

الأساسية في التشريعات الجزائية الإجرائية التي تقضي بأن الأصل في الإنسان براءته من التهمة المسندة إليه إلى ان تثبت إدانته بحكم قضائي قطعي.

المجرم في علم الإجرام

لقد واجه التعريف القانوني للمجرم انتقادات واضحة من بعض الفقهاء وعلماء الجريمة واستندوا في ذلك إلى عدة أسباب منها:

وجود طائفة من الأفعال المُجرمة قانونا ذات طابع إداري ولا يبرر وصف مرتكبها بأنه مجرم، مثل مخالفات المرور كإيقاف المركبة في مكان ممنوع، أوتجاوز الإشارة الضوئية وهي باللون الأحمر، فمثل هذه المخالفات لا ترقى بمرتكبها إلى مصاف المجرمين ما دام أن هذا السلوك لا يعبر عن عدم اكتراث حقيقي للنصوص القانونية المطبقة في المجتمع.

هناك الكثير من الأفعال التي يجرمها القانون الجزائي ويعاقب عليها لا تنم عن خطورة إجرامية ولا تعبر عن أي سلوك إجرامي، بل يُعد مرتكبيها في مصاف الابطال وليس المجرمين، مثل الجرائم السياسية، والاقتصادية، وجرائم الرأي، والجرائم ذات الصلة بحياة الفرد الشخصية وفي مجال حريته، في حين يعتبر الكثير من الناس أفعالا في دائرة التجريم على الرغم من عدم تجريم القانون لها، مثل الانتحار، الربا، الادمان على تعاطي المواد الكحولية، وهذه الأفعال تعد في نظر علماء الجريمة مهمة جدا لبيان مدى خطورتها وخطورة مرتكبيها ومن ثم محاولة القضاء عليها وكشفها للمشرع ليتدخل ويتناولها بالتجريم لما تشكله من خطورة واضحة على الفرد والمجتمع. (السراج، 1990، ص56).

لهذا فإن علماء الجريمة لا يتقيدون بالتعريف القانوني ويعتبرون الشخص مجرما طالما انه ارتكب فعلا مخالفا سواء نص عليه القانون أومن الأفعال المتعارف

والمتفق عليها من قبل المجتمع بأنها أفعال تقع في دائرة التجريم حتى لولم يصدر بحق الشخص حكم قضائي نهائي بذلك، فالمعيار للتجريم لديهم هوالفعل وليس الحكم فهناك الكثير من الأشخاص الذين يرتكبون أفعالا مجرمة قانونا ومجرمة اجتماعيا لكن لديهم القدرة الكافية لإقناع المحكمة أوالقاضي ونفي التهمة عنهم وبالتالي لا يصدر الحكم القضائي النهائي بحقهم فيترتب على ذلك خروجهم من دائرة التجريم، لهذا فإن المجرم في نظرهم هوكل شخص القي القبض عليه وتجري محاكمته أمام القضاء على فعل نص عليه القانون بالتجريم ولا يشترطون ثبوت الإدانة بحكم قضائي نهائي.

أنواع المجرمين وتصنيفاتهم

أولا: حسب نوع الجريمة

1- المجرمون المحترفين الممتنعين عن العمل: ويشتمل هذا الصنف على النشالين والعاهرات، والمتسولين والنصابين، وتجار الرقيق الأبيض، والمنجمين والمشعوذين والمهربين والمتلاعبين في السوق السوداء، والمجرمين الدوليين.

2- المجرمون المرتكبين لجرائم مالية بمقاومة خفيفة: هم الأشخاص الذين يتمتعون بمراكز اجتماعية محترمة، لكنهم يعجزون عن مقاومة مغريات الجريمة ودوافعها، ومن جرائمهم الاختلاس والائتمان التجاري وسرقة الأقارب والأموال العامة.

3- المجرمون المعتدين بالنفس: يتميزون بميل للحركة وقوى جسمانية مع ضعف في العواطف والإحساس، وانعدام الشعور الاجتماعي الرادع، ويطلق عليهم تسمية (لأشرار) ويلجأون لارتكاب الجرائم العدوانية؛ كالقتل والحرق والإيذاء الشديد، ويستعينون بالأسلحة غالباً في تنفيذ جرائمهم.

4- المجرمون ناقصي الكفاءة الجنسية: يشمل هذا الصنف العاجزين عن ضبط الغريزة الجنسية أومقاومتها، والشاذين جنسياً والساديين والملاوطين والموسوشيست الذين لا يجدون اللذة الجنسية إلا بالاعتداء عليهم، والممارسين مع الحيوانات والشبقيين (الفيتشت)، الذين يحصلون على شبعهم الجنسي من أشياء ترمز للجنس؛ كالثياب أوخصل الشعر أوالأحذية أوأدوات التجميل والزينة، تنحصر جرائم هذا الصنف في هتك الأعراض والجرائم المخالفة للآداب والمخلة بالحشمة كالاغتصاب واللواط ومواقعة المحرمات أوالأموات أومن كان فاقداً للوعي تحت تأثير مخدر أومسكر.

5- المجرمون الواقعون في أزمة: هم الأشخاص الذين يقعون تحت عبء أزمة متولدة داخل البيت أوالمجتمع ولا يستطيعون التغلب عليها إلا بالجريمة؛ كالنصابين والمحتالين على شركات التأمين والبنوك ويشمل المجرمين الذين يرتكبون جرائم الاعتداء كحرق البيت أوإتلاف الأثاث بسبب خلاف عائلي أوأزمة نفسية ويشمل الرجل الذي يقتل عشيقته تخلصاً من الحمل الحاصل نتيجة معاشرته لها، والمرأة التي تسقط حملها تخلصاً من عار الفضيحة أومن كثرة النسل.

6- مجرمي العقيدة: هم الأشخاص الذين يرتكبون الجريمة كواجب تفرضه عقديتهم دون التقيد بأحكام القانون الجنائي ويعلوفي نفوسهم واجب العقيدة على واجب احترام القوانين وتشمل جرائم هذا الصنف الجرائم السياسية والجرائم الإرهابية ويشمل هذا الصنف العاطفيين الذين يجدون في الجريمة تخفيفاً لآلام غيرهم كالأطباء وغيرهم الذين ينهون حياة مريض لا يرجى شفاؤه أومن ينهي حياة طفل مشوه بالخلقة لينقذه من عذاب المظهر طيلة حياته.

7- مجرمون متمردون على النظام العام: ويشمل الأشخاص الذين لا يقيمون وزناً للروابط الاجتماعية وللأنظمة والقوانين أوالمستهترين بالنظام والآداب كما يشمل

الأشخاص الذين يتعرضون لقيود اجتماعية أوسياسية أواقتصادية يفرضها نظام يختلف عما ألفوه سابقاً كما يشمل المسرحين من الجيوش إثر الحروب العالمية والذين يخلون بالأمن والنظام الجديد الذي يحرمهم من حرية التصرف والكسب.

8- مجرمين من غير الأصناف المذكورة سابقاً: ويشمل (المخاطرين دون ضمير الذين يرتكبون الجريمة دون وعي لنتائجها حتى تحقق غاياتهم كمروجي المخدرات - شهود الزور الطامعين بربح مادي - مرتكبي جرائم السلب والنهب)

ثانياً: تصنيف المجرمين حسب الأحوال المادية والاجتماعية:

ويشتمل على (المجرمين المحترفين والغير محترفين - المنحرفين والشواذ - الذهانيين والنفسيين)

ويمكن تقسيم أنماط الجريمة إلى مجموعة من الأنماط كما يلي:

الأنماط القانونية: التي تضع للمجرمين تصنيفات تستند إلى الفئات القانونية وتشير إلى الجريمة والمجرمين معا.

الأنماط النفسية: وتضع للمجرمين تقسيما في ضوء العوامل النفسية أوالسيكوباتية وتشير أساسا إلى المجرمين.

الأنماط التكوينية: وتستند إلى فكرة التكوين الجبري وتصنيف المجرمين استنادا إلى الوظائف البيولوجية النفسية.

الأنماط الاجتماعية: وتستند إلى تصنيف الظروف القائمة في المجتمع.

أنماط تستند إلى تعدد العوامل: وهي التي تجعل الرابطة التي تجمع فئة ما من الجرمين مجموعة من العوامل البيولوجية والنفسية والاجتماعية مستخدمة كل هذه العوامل في التصنيف وتشير أساسا إلى المجرمين.

أنماط المجرمين

لقد قسم علماء الجريمة الجرائم والمجـرمين إلى أصـناف وأنمـاط عديـدة بحسـب تكوينهم العضوي والنفسي والعقلي وبحسب الظـروف الاجتماعيـة والبيئيـة المحيطـة بهم، مما يؤثر على المسؤولية الجنائية لديهم ومن هذه التقسيمات أوالأنماط ما يلي:

تقسيم المجرمين إلى طائفتين هما المجرمين الأسوياء والمجرمين غير الأسوياء.

فالمجرمون الأسوياء هم من تتوافر فيهم كافة شروط المسؤولية الجنائية لخلـوهم من العوارض التي تؤثر على سلامة إدراكهـم واختيـارهم، وبعبـارة أخـرى هـم الـذين يتمتعون بالقدرة على الإدراك أوالوعي من ناحية، ولديهم حرية الاختيـار مـن ناحيـة أخرى، فهم لا يختلفون عن عامة الناس وإن وجد هذا الاخـتلاف فهوطفيـف لا يـؤثر في قدرتهم على الإدراك والاختيار وهؤلاء يسألون عن تصرفاتهم جنائياً.

أما المجرمون غير الأسوياء فهم على نوعين: مجرمون مجانين ومجرمون شواذ، أمـا المجرمون المجانين فهم المصابون بمرض من الأمراض العقلية والـذي يـؤدي إلى تخلـف ملكة الوعي وحرية الاختيار لديهم فتنعدم المسؤولية الجنائية بسبب ذلـك، وتسـقط عنهم العقوبات المقررة في القانون، وهذا لا يمنع من اتخاذ بعـض التـدابير الاحترازيـة بحقهم لمواجهة الخطورة الإجرامية لديهم والعمل على إيجاد علاج لهم.

أما المجرمون الشواذ فهم الأشـخاص المصـابون بخلـل جـزئي في تكـوينهم العقـلي أوالـنفسي أوالعضـوي، وهـذا الخلـل لم يصـل إلى الحـد الـذي تنعـدم فيـه أهليـتهم ومسؤوليتهم الجنائية، فهم يحتلون طائفة وسطى بين طوائف المجرمين، إذ يتمتعـون بقدر من الإدراك والاختيار أقل من ذلك الـذي يتمتـع بـه المجرمـون الأسـوياء، وأكـثر

مما لدى المجرمون المجانين، وهؤلاء تقـرر لهـم بعـض التشريعـات مسـؤولية جنائيـة مخففة. (يسر، 1999، ص 98)

لقد اختلف علماء الجريمة حول أي من هـذه الفئـات الـذين يجـب ان تشـملهم دراسات علم الإجرام حيث كان هناك ثلاثة اتجاهات حول هذه الموضوع وهي:

- **الاتجاه الأول:**

حاول أصحاب هذا الاتجاه اقتصار دراسات علم الإجـرام عـلى المجـرمين الأسـوياء دون غيرهم، لأن هؤلاء المجرمين هم وحدهم الـذين يسـألون مسـؤولية جنائيـة عـن أفعالهم وتصرفاتهم، فالجريمة هي سـلوك أوفعـل يجـب معاقبـة ومسـائلة الشـخص الذي يرتكبها في حال ان يكون متمتعا بالأهليـة والإدراك والإرادة، أمـا المجنـون الغـير عاقل فهولا يسأل عن أفعاله ولا يعـد جريمـة في نظـر القـانون، إضـافة إلى أن سـلوك المجرم غير السوي معلوم السبب وينشغل بدراسة البحث فيه علم الطب العقـلي ولا علاقة لعلم الإجرام به. (ابوعامر وفتوح، 2000، ص44).

- **الاتجاه الثاني:**

يدعوأنصار هـذا الاتجـاه إلى اقتصـار دراسـات علـم الإجـرام عـلى المجـرمين غـير الأسوياء بحجة أن هؤلاء المجرمين يرتكبون جرائمهم بسبب عوامـل نفسـية أوعضـوية أوعقلية، لذلك يجب ان تكون اهتمامـات هـذا العلـم في البحـث عـن حقيقـة هـذه العوامل، أما بالنسبة للمجرمين الأسوياء فمن وجهة نظرهم يجب ان تتولى دراسـتهم علوم أخرى مثل علم الاجتماع الجنائي وعلم النفس الجنائي أوعلم النفس العـام، مـن أجل معرفة العوامـل الحقيقيـة الدافعـة إلى الإجـرام كـالمجرم بالصـدفة الـذي تقـف العوامل الاجتماعية أوالبيئية وراء إجرامه (الصيفي، 1998 ص92).

- **الاتجاه الثالث:**

هذا الاتجاه يؤكد على وجوب شـمولية علـم الإجـرام في دراسـاته عـلى المجـرمين الأسوياء وغير الأسوياء لعدة أسباب منها:

صعوبة التمييز بين المجرم السوي وغير السوي، فليس من السـهل تحديـد درجـة الأهلية التي يعـد الفـرد عنـدها سـوياً، وبالتـالي يمكـن القـول أنـه يصـلح لان يكـون موضوعا لعلم الإجرام فكافـة الأفـراد سـواء كـانوا مجـرمين أم غـير مجـرمين يعـتريهم النقص في صحتهم النفسية والجسدية، والشخص السوي لا يـبرأ مـن هـذه النـواقص، وإنما تكون هذه النواقص في أدنى درجاتها بحيث يمكن السيطرة عليهـا، وبالتـالي فـإن الخلاف بين المجرم السوي وغير السوي يمكن رده إلى مقدار هـذه النقـائص أي فـارق كمي، ولذلك لا يمكن اقتصار دراسات علم الإجرام فقـط عـلى المجـرم السـوي. (عبـد المنعم، 2003، ص 116).

ليس صحيحا ان فعل غير الأسوياء لا يعد جريمة في نظر القـانون، فهـم يرتكبـون أفعالا ينطبق عليها وصف الجريمة، وإذا كان القانون يخـرجهم مـن دائـرة المسـؤولية الجنائية فهذا لا ينفي عنهم صـفة الإجـرام، والـدليل عـلى ذلـك ان العلـماء يطلقـون عليهم تسمية المجرمون غير الأسوياء، ومن ناحيـة أخـرى فـإن هـؤلاء المجرمـون وإن كانوا يفلتون من العقوبة لأنهم غير أهل لتحملها فان القانون يخضعهم لصورة أخرى من صور الجزاء التي تتمثل في التدابير الاحترازية، ولا يمكن لعلماء الإجرام تحديـد مـا يناسبهم من هذه التدابير بمعزل عن دراسة جرائمهم والدوافع التي أدت إلى ارتكابها(الوريكات، 2009، ص61)

لا يمكن التسليم بأن إجرام غير الأسوياء يعود لما أصابهم من خلل عقـلي أونـفسي باعتباره السبب الوحيد الذي يكمن في تفسير إجرامهم، فلم يقم الدليل عـلى ان كـل مـريض بـالجنون أوبخلـل في قـواه العقليـة أوالنفسـية يعـد مجرمـاً، ولوصـح ذلـك

لوجب ان يجرم جميع الأشخاص غير الأسوياء، ولكن الحقيقة تشير إلى أن بعض هؤلاء فقط هوالذي يرتكب الجريمة، الأمر الذي يستلزم البحث عن العوامل الأخرى التي دفعت بهذه الطائفة إلى التردي في مهاوي الجريمة، والبحث عن هذه العوامل من صميم اختصاص علم الإجرام الذي يتعين عليه استظهارها (الشاذلي، 2006، ص30).

لهذا ومن خلال ما تم استعراضه يمكن القول بأن مسؤولية علم الإجرام هي دراسة كافة أنماط وفئات المجرمين سواء كانوا أسوياء أم غير أسوياء حتى لولم تلحقه المسؤولية الجنائية على الأفعال التي يرتكبها بسبب حالته المرضية ومعرفة الدوافع والعوامل التي أدت إلى ارتكاب تلك الأفعال والجرائم وهذا ما يفيد كل من المشرع والقاضي والجهات التنفيذية في اتخاذ كافة الوسائل والبدائل المتاحة للتعامل مع هؤلاء الأشخاص من اجل حماية المجتمع.

أما لومبروزو1876م فقد وضع تقسيما للمجرمين بناء على ما تم دراسته من المجرمين الذين تعامل معهم من خلال خدمته كطبيب في الجيش حيث تمكن من تشريح جثث بعض المجرمين فخلص إلى تصنيفات معينه منهم المجرم بالميلاد والمجرم الصرعي والمجرم المجنون والمجرم العاطفي وغيرها من التصنيفات أما جارفيلوفقد وضع تقسيما رباعيا للمجرمين هم:

- المجرم القاتل
- المجرم العنيف
- المجرم السارق الذي يفتقر إلى الأمانة والنزاهة
- المجرم الفاسد جنسيا.

وأما العالم فيري فقد اجرى تعديلات على نظرية لمبروزووخلص إلى التصنيفات التالية للمجرمين: (الوريكات، 2009، ص90-92).

- المجرم بالفطرة أوالمجرم بالميلاد:

وهوالمجرم الذي يتميز بملامح عضوية وصفات نفسية موروثة يرتد بها إلى عهد الإنسان البدائي الأول، ومن هذه الصفات ما هوعام ومشترك بين جميع المجرمين، ومنها ما هوخاص بجرائم معينة على النحوالذي بيناه من قبل.

- المجرم المجنون:

وهوالشخص الذي يرتكب الجريمة تحت تأثير المرض العقلي الذي أصابه، ويدخل "لمبروزو" في هذه الفئة أيضا المجرم الهستيري ومدمن الخمور والمخدرات.

- المجرم الصرعي:

وهوالشخص المصاب بصرع وراثي، ويؤثر هذا المرض على العضلات والأعصاب والحالة النفسية والعقلية للمصاب به، وقد تتطور حالة الصرع أوتزداد مضاعفاته لديه، فيتحول إلى مرض عقلي، ويصبح المجرم الصرعي مجرما مجنونا لا مجرما صرعيا، وقد توصل "لمبروزو" إلى علاقة الصرع بالإجرام لدى فحصه حالة المجرم "مسديا" كما ذكرنا أنفا.

- المجرم السيكوباتي:

وهوالشخص الذي يعجز عن القدرة على التكيف مع المجتمع نتيجة الاضطرابات السلوكية التي تصيب النواحي المزاجية لديه، فلا يستطيع ان يسلك

سلوكا قويما في المجتمـع، فيتصـادم معـه، ولا يكـون أمامـه إلا الانـزلاق نحوالجريمـة، ويطلق على هذه الحالة أيضا وصف المجنون خلقيا.

- المجرم المعتاد:

وهوالذي يولد دون ان يحمل صفات المجرم بالفطرة أوالميلاد - كما يرى "لمبروزو" – وإنما تغرس فيه النزعة الإجرامية أوالميل إلى ارتكاب الجريمة نتيجة الظروف البيئية المحيطة به، ويعتبر الإجـرام بالنسـبة لـه حرفـة أوطريقـة حيـاة، فإجرامـه عـلى هـذا النحومكتسب لا بالميلاد.

- المجرم العاطفي:

وهوالمجرم الذي لا يرتكب الجريمة بسبب تكوين وراثي خاص به أوضعف في قواه العقلية، وإنما لأسباب عاطفية خالصة كالحماس الزائد أوالغـيرة المفرطـة أوالاسـتفزاز، فهوإنسان يتمتع بشعور مرهف وحساسية بالغة لا يمكـن مقاومتهـا وبالتـالي ينـدفع تحت تأثيرها لارتكاب الجريمة، كالحب والغيرة والحماس لموقف أورأي معين، والدفاع عن العرض أوالشرف، ومعظم الجرائم التـي يرتكبهـا هـذا النـوع مـن المجـرمين هـي جرائم اعتداء على الأشخاص أوجرائم سياسية.

- المجرم بالصدفة أوالمجرم العرضي:

وهوالشخص الذي لا يسـعى للجريمـة، وإنمـا يقـع فيهـا بسـبب عوامـل خارجيـة عارضة، ويمكن ان تنقسم هذه الفئة من المجرمين إلى نوعين:

المجرم الحكمي: وهوالشخص الـذي يرتكـب جريمـة شـكلية، أي جريمـة يعتبرهـا القانون كذلك، وان تجرد السلوك فيها من أي خطورة إجرامية لـدى الفاعـل، ومثالهـا جرائم حمل السلاح بدون تـرخيص، بعـض الجـرائم الاقتصـادية، جـرائم الصـحافة أو الرأي.

المجرم المريض بالإدمان: وهوالشخص الذي أدمن على تناول المسكرات أوتعـاطي المخدرات، بحيث يؤدي هذا الإدمان إلى إضعاف ضوابط سلوكه، ويصبح أكـثر عرضـة لارتكاب الجريمة التي قد لا يرتكبها الأفراد العاديين من غير المجرمين، أي ان الحادثـة البسيطة التي لا تدفع غيره إلى الجريمة تكفـي وحـدها لان تدفعـه إلى سـلوك سـبيل الجريمة، وهذا المجرم يحتل من حيث الخطورة مركزا وسطا بين المجرم بالميلاد والرجل العادي، إلا انه قد يتحول إلى مجرم معتاد إذا طالـت مـدة إقامتـه بالسـجن واخـتلط بالمجرمين الآخرين ولا سيما العتاة منهم.

المبحث الثالث : الظواهر الإجرامية مفهومها وعناصرها وانواعها وخصائصها ، والجرائم المستحدثة مفهومها وخصائصها واثارها:

الظواهر الإجرامية

تثير الظاهرة الجرمية اهتمام الانسان منذ قديم الزمان، حيث تشير الجريمة إلى الصراع ما بين الخير والشر، وهذا الصراع مسألة حتمية وُجد قبل خلق الإنسان، حيث كانت الجرائم موجودة قبل ذلك، إلا أن الاستدلال الدائم للجرائم التي وقعت على وجه الأرض بدأت عندما قتل قابيل أخيه هابيل، وهي الجريمة الأولى التي وقعت على الأرض ثم بدأت الجرائم تنتشر بسبب التكاثر البشري وتطور المجتمعات.

فالجريمة توصف بأنها تعدي واضح على الحياة الاجتماعية القائمة على فكرة التعاقد والتضامن بين أفراد المجتمع، إضافة إلى أن الجريمة لها آثارها الضارة على التوازن في المجتمع وتمثل خطراً يهدد القيم والمصالح المجتمعية.

ولذلك فالظواهر الإجرامية تعتبر ظواهر حقيقية وواقعية، ولها أبعادها التاريخية، وهي صفة ملازمة للإنسان، فالأصل في الانسان أن يتصف بالسلوك السوي المستقيم، لكن النفس البشرية يتنازعها الخير والشر، ولهذا فالجريمة موجودة في كل المجتمعات البشرية وهي ممتدة ومتطورة بتطور الحياة البشرية وبما يحققه الانسان من تقدم علمي وتكنولوجي.

حدد علماء الاجرام بأن أفضل الوسائل لمواجهة الظواهر الإجرامية هومعرفة العوامل المؤدية لها ودراستها دراسة شاملة من جميع الجوانب، فعلم الاجرام

هوالعلم الذي يـدرس الظـاهرة الجرميـة مـن كافـة جوانبهـا؛ النفسـية والاجتماعيـة، والثقافية، والسياسية، والاقتصادية، والقانونية وغيرهـا وتحديـد العوامـل المؤديـة لهـا بأسلوب علمي للوقاية منها ومنع انتشارها والحد من مخاطرها، لتسهيل القبض عـلى مرتكبيها وايداعهم للجهات المختصة لنيل العقوبة المستحقة عليهم.

مفهوم الظاهرة الجرمية

اعتمدت الدراسة المفهوم الإجرائي للظاهرة الجرميـة وهـي: العمليـات التـي يـتم فيها ارتكاب الجريمة بصورة متكـررة ومنتظمـة الوقـوع في نـوع معـين مـن الجـرائم، وترتكب بأسلوب جرمي واحد، وفي منطقة أوبقعة جغرافية، وخـلال فـترات متعاقبـة من الزمن، وترتكب من قبـل جماعـة إجراميـة أوعـدة جماعـات تتصـف بالبراعـة في ارتكاب تلك الجرائم.

عناصر الظاهرة الإجرامية

يمكن القول ومن خلال ما تم استعراضه من مفهوم الظاهرة الجرميـة بأنـه لا بُـد من توافر العناصر التالية في الفعل الجرمي ليكون ظاهرة جرمية وهي:

- التكرار: ويعني تكرار الفعل الجرمي، وهومن العناصر الجوهريـة حيـث لا يمكـن وصف الظاهرة الجريمة بأنها ظاهرة من خلال فعل جرمي واحد وغير مكرر.
- تكرار نفس الفعل الجرمي: أي أن يكون ارتكاب فعـل جرمـي معـين مكـرراً أوأن يكون هناك تشابهاً في ارتكاب الجريمة بحيث يمكن وصـفها بأنهـا جريمـة واحـدة لشدة تماثلها، وحتى يتحقق التماثل في الفعل الجرمي يجب توافر شرطين هما:
- وحدة محل الجريمة: وتعني أن يكون محل الجريمة واحداً، مثل أن تقـع الجريمـة على الإنسان أوعلى المنازل، أوعلى البنوك، أوعلى كبار السن، أوالفتيات.

- وحدة المشروع الإجرامي: وهويعني أن يكون المشروع واحداً مثل الخطف، القتل، اغتصاب الفتيات، الاتجار بالأطفال وغيرها من الجرائم.
- وحدة أسلوب ارتكاب الجريمة: بمعنى أن يكون الأسلوب المرتكب في الجريمة موحداً في كل جريمة يتم ارتكابها، حيث يكون لكل مجرم أوجماعة إجرامية بصمتهم واسلوبهم الخاص بهم تميزهم عن غيرهم من المجرمين.

ويتحدد أسلوب الجريمة من خلال عدة معايير منها:

- موضوع الجريمة: مثل ظاهرة السطوعلى البنوك المصارف، أوالسرقة المقرونة بالتهديد أوالقتل، أوجرائم الاختلاس والرشوة وغيرها.
- وقت ارتكاب الجريمة: غالباً ما يتم ارتكاب الجرائم من قبل الأشخاص ذوي الأساليب الجرمية المحددة في أوقات محددة وذات طابع معين مثل الوقت المتأخر من الليل، أوساعات النهار المبكرة، أوأثناء المناسبات المختلفة وغيرها. ومن سمات الظاهرة الإجرامية أن يكون الفارق الزماني بين ارتكاب الجرائم قريباً اومتقارباً وعند انتظام وقت ارتكاب الجرائم قد تكون المخاطر أكثر.
- مكان ارتكاب الجريمة: عادة ما يرتبط أسلوب ارتكاب الجرائم بأماكن محددة مثل؛ المتاجر، الأماكن المزدحمة، الطرق الغير مأهولة، المنازل وغيرها.
- أداة الجريمة: يعتمد كل مجرم على أداة محددة لتنفيذ جريمته فتكون هي الأداة المفضلة لديه، مثل السلاح الناري، السموم، الحبال، الأدوات الحادة، المواد الكيماوية وغيرها.
- المظهر الخاص بالجاني: فالجاني يحاول دائما الاهتمام بمظهره حسب الحالة الجريمة التي يريد ارتكابها لعدة أسباب منها التمويه على الآخرين لإقناعهم بأنه

نفس الشخصية التي يمثلها كالتاجر أورجل الاعمال أوالسياسي وغيرها، وكذلك البعض يلجأ لتغيير مظهره ليظهر كرجل دين أوشخص محتاج لينال عطف الناس عليه.

- شركاء الجاني: غالباً ما يكون هناك شركاء للجاني عند ارتكاب الجريمة، خاصة الظواهر الجرمية المتكررة، فلا يعقل أن يتم ارتكاب جرائم متكررة وفي أوقات زمنية محددة وأماكن معينة من قبل شخص واحد، فقد يكون هؤلاء شركاء رئيسيين في ارتكاب الفعل الجرمي، وقد يكونون تبعيين إما للتمويه وإما للتغطية على الجاني أولتقديم الدعم والمساندة له بطريقة غير مباشرة.

- قصة الجاني: يستخدم كل مجرم قصة أوقصص خاصة عند ارتكاب الجرائم اوالتمهيد لارتكابها، فمثلا جرائم النصب والاحتيال تحتاج إلى لعب بعض الأدوار من الجاني أوالجناة لإقناع الضحايا بهم، فقد يكون المظهر العام لهم مثل اللباس وتوفر المال، والسيارات الفاخرة مثلا وغيرها، وفي بعض الأحيان يلعب الجاني دور رجل الاعمال ليقوم بإيهام الآخرين بمشاريعه التجارية كتغطية لغسل الأموال أوالاتجار بالبشر أو الاتجار بالمخدرات وغيرها، وفي بعض الأحيان تكون قصة الجاني تتمثل بادعاء المرض للحصول على المال، أوالادعاء بأنه رجل أمن أوطبيب وغيرها من المهن.

- طريقة ارتكاب الجريمة والهروب من المكان: لكل مجرم بصمته واسلوبه الخاص بارتكاب الجريمة، فمن يرتكب جرائم السرقة مثلا يقوم بالكسر والخلع، اواستخدام المفاتيح المتعددة، اوالدخول عبر النوافذ اوأسطح المنازل، وفي بعض الجرائم قد يستخدم المجرم طرق مختلفة مثل التخدير أوالعنف والتخفي بملابس وأقنعة وغيرها.

خصائص الظاهرة الإجرامية:

تتميز الظواهر الإجرامية بعدد من الخصائص كما يلي:[1]

- الجريمة مشروع إجرامي يتميز بالاحترافية: فالجاني الذي يقوم تكرار الجريمة في أماكن وأوقات منتظمة يتميز بأنه مجرم محترف ويؤدي عمله الإجرامي بطريقة تجعل من الصعوبة ضبطه بسهولة.

- تتميز الجريمة بالتنظيم: أي أن لها تنظيماً إداريا ومالياً وتخطيطاً مسبقاً، وقد يكون هذا التنظيم بدائياً أوعلى درجة من التطور من خلال استخدام التقنية الحديثة في ارتكاب الجرائم، وفي مثل هذا النوع يتم توزيع الأدوار بين أفراد الجماعة الإجرامية، مثل جمع المعلومات، المراقبة، التنفيذ، الاستلام، التوزيع، إخفاء محل الجريمة وغيرها.

- الظاهرة الجريمة مشروع يقوم على توظيف المهارات الخاصة: حيث يتمتع الجاني أومجموعة الجناة بنوع من المهارة والبراعة ويتميز بعضهم بالذكاء الحاد، والمعرفة العليمة، فمثل هؤلاء الأشخاص لديهم القدرة على الابتكار الذي قد يحير رجال التحقيق والأمن في بعض الأحيان، فعند ارتكاب بعض الجرائم تكون الحاجة للأشخاص الأذكياء ومن لديهم القدرة على الابتكار مثل التزوير مثلا، اوخبراء في الحاسوب والقرصنة، وبعضهم يكون لديه القدرة على تصنيع الأسلحة بطرق ابتكارية ولها فعالية مثل المتفجرات أوبعض الأسلحة القاتلة، كذلك الحال في الاستثمارات المالية والمصرفية وغيرها.

ويمكن القول بأن مرتكبي الجرائم الإلكترونية لديهم قدرة وتدريب ومهارة عالية في ارتكاب هذه الجرائم، لأن الاستيلاء على المعلومات أوالدخول إلى بيانات الأفراد اوالشركات أوالمصارف فهذه الجرائم لا يستطيع أي شخص القيام بها وانما

(1) المرشدي، أمل (2016) الظاهرة الإجرامية، موقع محاماة نت متوفر عبر الرابط: https://www.mohamah.net/law

تحتـاج إلى أشـخاص ذوي مهـارات عاليـة، وهـذه الجـرائم تلحـق الضرر والخسـائر الاقتصادية الكبيرة سواء على الأفراد اوالمؤسسات أوالدول، إضافة إلى صعوبة التعـرف على الجاني أوضبطه.

الظاهرة الجرمية لها تأثير على الحياة الاجتماعية في المجتمع: فالجريمة قـد تهـدم القيم الاجتماعية وتنشر الفوضى في المجتمع، وتزيد من مستوى الخوف لـدى الأفـراد، وتقلل فرص التنمية في المجتمع.

الظهور المفاجئ: من خصائص الظـواهر الجرميـة أنهـا تظهـر فجـأة مـما يجعلهـا محط اهتمام الناس بها وتزيد من معدل الخوف وعدم الشعور بالأمان في المجتمع.

الظواهر الإجرامية تتميز بالوضوح: فهي ظواهر واضحة للجميع وتثير شـكواهم وتزيـد مـن مخـاوفهم؛ مثـل جـرائم الإرهـاب مـثلاً اوجـرائم السـلب عـلى الطرقـات الخارجية وجرائم خطف الأطفال وغيرها.

تحديد الأهداف: فالظواهر الإجرامية لهـا أهـداف محـددة؛ مثـل الحصـول عـلى المال، نشر الرذيلة في المجتمع، نشر المخدرات، سرقة المنازل، وقـد يكـون الهـدف مـن وراء ارتكاب الجرائم ذوطابع ديني أوسياسي أواقتصادي اوثقافي.

زيادة عدد الضحايا: إن التكرار المستمر في ارتكاب الجرائم حتماً سينج عنه زيادة في أعداد الضحايا والمجني عليهم، وغالباً ما تكون الفئـات الضـعيفة في المجتمـع هـم الغالبية العظمى من الضحايا مثل الأطفال والنساء وكبار السن.

الخطورة الإجرامية: تتميز الظواهر الإجراميـة بأنهـا ذات خطـورة عـلى المجتمـع، فهي تشـكل خرقـاً للقـانون والنظـام والأمـن العـام في الدولـة، وتعمـل عـلى زعزعـة الاستقرار فيه، وهذه النتائج قد تؤدي إلى تدهور الاقتصـاد في الدولـة وانهيـاره، وقـد تؤدي إلى التفكك الاجتماعي وانتشار الفوضى في المجتمع.

القدرة على الانتشار والامتداد الجغرافي: تتصف الظواهر الإجرامية بأن لديها القدرة على الانتشار والانتقال من مكان لآخر بسرعة، فالجرائم في عصر التقنية الحديثة أصبحت عابرة للقارات ولا يمكن التصدي لها بالوسائل التقليدية كما هوالحال في جرائم الإرهاب وتجارة المخدرات والاتجار بالبشر وغسل الأموال وغيرها.

وبهذا نرى بأن الظواهر الإجرامية تشكل خطراً على المجتمعات وتنشر الرعب والخوف فيها خاصة في ظل انتشار الجرائم عبر التقنيات الحديثة وبرامج الذكاء الاصطناعي، فقد أصبح انتشار هذه الجرائم يشكل مخاطر كبيرة على المجتمعات، لذا لا بُد من القيام بعمليات استشراف للمستقبل وتوقع نوع الجرائم المحتمل ظهورها وانتشارها في المستقبل وبناء الخطط الاستراتيجية لمواجهتها والتصدي لها.

أنواع الظواهر الإجرامية

تختلف أنواع الظواهر الإجرامية بحسب تبعاً للمعايير التي تستند إليها وتعتمد عليه في تكوينها ومنها:

- الظواهر الإجرامية بحسب النشاط الجرمي: وهذا النوع من الظواهر هوالأكثر شيوعاً، حيث يتم وصف الظاهرة بالفعل الجرمي مثل ظاهرة المخدرات، وظاهرة سرقة السيارات وغيرها.

- الظواهر الإجرامية حسب مكان ارتكابها: فالظاهرة الجرمية قد تكون محصورة بمكان جغرافي محدد مثل ظاهرة الثأر التي تنحصر في مجتمعات محددة ولا توجد في مجتمعات أخرى في نفس الدولة، وقد تكون شاملة لكافة حدود الدولة مثل المخدرات، والجرائم الإلكترونية، والسرقة وغيرها.

- الظواهر الجرمية بحسب زمن ارتكابها: وهي الظواهر التي ترتبط بأوقات محددة مثل؛ سرقة المنازل في الصيف، حيث يتركها أصحابها في فترات معينة إما للتنزه أوللسفر، فتكون بذلك عرضة للسرقة، وهناك بعض الظواهر التي تسمى بالظواهر الموسمية وهي التي تكون مرتبطة بموسم معين مثل الصيف والشتاء، موسم قطاف الثمار وغيرها.

- الظواهر الإجرامية بحسب الدافع على ارتكابها: قد يكون وراء ظهور بعض الظواهر الإجرامية عوامل عديدة تؤدي إلى انتشارها منها؛ نشر الفوضى الاجتماعية نتيجة عدم العدالة الاجتماعية أوالظروف الاقتصادية الصعبة.

- المنافسة الاقتصادية بين الشركات والبنوك، فقد تنتشر ظاهرة السطوعلى البنوك أوالمحلات التجارية الكبرى بقصد التأثير على تلك المؤسسات لغايات المنافسة التجارية والاقتصادية.

- زعزعة الأمن العام وهذا النهج يستخدمه الخارجين من السجون بهدف زعزعة الاستقرار والأمن في المجتمع وفي بعض الأحيان يكون الهدف منها هوخلق عصابات إجرامية تسهل عمليات السطووالسرقة وأخذ مبالغ مالية من أصحاب المصالح مقابل عدم التعرض لهم وحماية مصالحهم من أي اعتداء.

- الظواهر الإجرامية العارضة: وهي الظواهر التي تظهر فجأة وتختفي بسرعة مثل ظاهرة خطف الأطفال، وظاهرة السطوعلى الصيدليات للحصول على المواد المخدرة، وبعض أنشطة العصابات الإجرامية التي سرعان ما تنشر هذه السلوكيات وعند تحقيق أهدافها تختفي بسرعة.

التمييز بين الظواهر الإجرامية والجرائم التقليدية

تُعرف الجريمة العادية بأنها مشروع إجرامي يبدأ من لحظة البدء بالتنفيذ وتنتهي عند الانتهاء منه والقيام بكافة الوقائع المكونة لهذه المشروع، ولا يشترط فيها التكرار كما هوالحال عند تعريف الظاهرة الإجرامية ولا يشترط الاستمرارية، فالجريمة التقليدية ترتكب من فاعل واحد أوعدد من الفاعلين، ويكون الضحايا فيها ضحية واحدة أوعدد من الضحايا، ومن أوجه التمييز بين الجرائم التقليدية والظواهر الإجرامية ما يلي:

- يُشترط في الظاهرة الإجرامية التكرار والاستمرارية في التنفيذ مثل جرائم السرقة المتكررة، سرقة السيارات، السطوعلى البنوك، الخطف، في حين أن بعض الجرائم وان تكررت لا تعتبر ظاهرة مثل استخدام أوراق مزورة من قبل شخص لعدة مرات، جريمة قتل شخص لعدة أشخاص في وقت واحد.

- ضحايا الجرائم التقليدية في الغالب على ضحية واحدة أوعدد محدود من الضحايا، أما الظاهرة الإجرامية فهي تقع على عدد كبير من الضحايا وغير محددين مسبقاً.

- العنصر الزماني والمكاني للجريمة التقليدية يكون قريب من الفعل الجرمي حيث ينتهي المشروع الجرمي بانتها الأفعال التي يتكون منها، أما الظاهرة الجرمية فهي غير محدودة بزمان ومكان معين أي أنها تكون في أوقات مختلفة وفي أماكن جغرافية أكثر وأوسع.

- الجريمة العادية اوالتقليدية غالباً ما تكون فردية الارتكاب وليس لها صفة الديمومة فهي تنتهي بانتهاء الفعل، أما الظاهرة نادراً ما تكون فردية، وفي الغالب هي مشروع جماعي يتصف بالديمومة ويدخل التنظيم والاحتراف في تنفيذها.

الجرائم المستحدثة

ظهرت في العقود الماضية العديد من أنماط الجرائم الحديثة أوالمستحدثة على المستوى العالمي سرعان ما انتقل إلى المستويات المحلية والإقليمية، وهذه الجرائم تختلف عن الجرائم التقليدية المألوفة للناس، فهي تستخدم التكنولوجيا الحديثة في ارتكابها مما يجعل من مواجهتها وملاحقة مرتكبيها أمراً في غاية الصعوبة خصوصاً وان الجريمة ترتكب من مكان خارج الحدود الوطنية للدولة، وهذه الجرائم تسعى لتحقيق أهداف مختلفة ذات طابع إجرامي منظم، وفيها تقاسم في الأدوار(اليوسف، 2004)

والظواهر الإجرامية المستحدثة أوما تسمى بالجرائم المستجدة هي جرائم ظهرت نتيجة التغير الذي حصل في المجتمعات بشكل عام، ونتج عنها التغير في أنماط ووسائل العيش، والتحول في الحياة البشرية المعاصرة في جميع المجالات؛ الاقتصادية، الاجتماعية، السياسية، والثقافية وغيرها، وهذه الجرائم تختلف عن الجرائم التقليدية المعروفة لدى الجميع، فهي تتصف بالخطورة العالية والدقة في التنفيذ لاعتمادها على التقنيات الحديثة في تنفيذها.(الخليفة، 1999)

وقد برز مصطلح الجرائم المستحدثة منذ تسعينيات القرن الماضي في ظل انتشار بعض الأنماط الجديدة من الجرائم التي لم تكن موجودة في المجتمعات سابقاً، وقد أخذ هذا المفهوم العديد من المسميات المرادفة لمفهوم الجرائم المستحدثة مثل؛ الجرائم المعاصرة، والاجرام المعاصر، أوقضايا أمنية معاصرة، وغيرها من المسميات التي تدل على معنى واحد وهوجرائم ترتكب بطرق غير تقليدية(البشري، 2004)

ويشير مصطلح الجرائم المستحدثة إلى أنماطاً جديدة من الجرائم، وتعتمد على أساليب وأدوات في تنفيذها، حيث ورد تعريفها على أنها نمط من الجرائم الغير مألوفة في المجتمع، ولها أسلوب خاص في تنفيذها، ونوع الجرائم المرتكبة وكذلك

حجم تلك الجرائم، كما ورد معناها في أنها تلك الجرائم التـي تعتمـد عـلى التخطـيط بالاعتماد على التقنيـات الحديثـة واسـتخدام الحاسـب الآلي، وهنـاك مـن يقـول أنهـا جرائم عادية لكنها تستخدم التقنية الحديثة من أجل إخفاء معـالم الجريمـة وتسـهيل عملية تنفيـذها، وورد معناهـا بأنهـا نمـط مـن الجـرائم أوالسـلوكيات الخارجـة عـن القانون، ولم يألفها المجتمـع مـن قبـل، وتسـتخدم التكنولوجيـا الحديثـة في ارتكابهـا، وينتج عنها أضراراً متعددة.

مفهوم الجرائم المستحدثة

تناول الباحثون والخبراء مفهوم الجـرائم المسـتحدثة مـن زوايـا عديـدة للإحاطـة بالمفهوم الشامل للمعنى الذي يشير إلى الجرائم المستحدثة ومن هذه التعريفات:

هي الجرائم التي يتم التخطيط لها، ويستفيد المجرمون من التكنولوجيا الحديثـة في ارتكابها مثل؛ جرائم الإرهاب، والمخدرات، والاحتيال الإلكـتروني، وجـرائم الحاسـب الآلي، وغيرها.

وتعرف على أنها الجرائم التي لم تكن مألوفة في المجتمع سابقاً، نتيجـة التطـور في استخدام التقنيات الحديثة.

وعرفت على أنها الجرائم التي لم يكن لها تشريع سابق ينظمها من قبل.

وبناء عـلى هـذه التعريفـات يمكـن القـول بـأن الجـرائم المسـتحدثة تقـوم عـلى مجموعة من العناصر منها:

- أنها جرائم لم تكن معروفة أومألوفة سابقاً لدى الناس.

- تستخدم التقنية الحديثة في تنفيذها بشكل كامل.

- لا يوجد لها تشريعات محددة وواضحة.

لا تعتمد على العنصر المكاني في ارتكابها بمعنى لا تشترط لارتكابها وجود الجاني في المكان أوالهدف المستهدف.

تعتمد على مجموعة من المعايير لتصنيفها بالجرائم المستحدثة مثل المعيار الاجتماعي أي التغيير في البنية الاجتماعية للمجتمع، والمعيار القانوني، وهوعدم وجود نص تشريعي يجرم الفعل ويعاقب مرتكبه، والمعيار الاجرائي وهوالحداثة في طريقة ارتكاب الجريمة أوالهروب والافلات من الملاحقة الأمنية والقضائية.

خصائص الجرائم المستحدثة

تتميز الجرائم المستحدثة بالعديد من الخصائص التي تميزها عن الجرائم التقليدية، والمقصود بالخصائص هوالوصف الدقيق لها، ومعرفة الظروف التي أدت لظهور مثل هذه الجرائم، ومعرفة أنماطها، والخسائر المترتبة عليها، ومن هذه الخصائص ما يلي: (الردايدة، 2013)

- الجرائم المستحدثة متعددة الأسباب ومتنوعة في الآثار، وهي تشكل خطراً على الأمن العام للمجتمعات، وتهدد الحياة فيها، وتعمل على التغيير في البنى الاقتصادية والاجتماعية، وهي تتطلب معرفة علمية تامة لوصفها وتحديد مكامن الخطورة فيها.

- الجرائم المستحدثة جاءت نتيجة الثورة التكنولوجية والتطور في التقنيات الحديثة، مما ساعد على ارتكاب بعض الجرائم بفضل تلك التقنيات.

- التحرر من خصوصية الزمان والمكان عند ارتكاب الجرائم، حيث أصبحت هذه الجرائم ترتكب في أماكن تختلف عن أماكن تواجد الجناة، لهذا اصحبت هذه الجرائم تأخذ صفة الجرائم الدولية حيث انتقلت من المحلية إلى العالمية العابرة للحدود.

- الجناة في الجرائم المستحدثة قد يكونوا متعددي الجنسيات، مما يجعل من ملاحقتهم قضائياً وأمنياً أمراً في غاية الصعوبة، وهذا يساعد على ارتكاب المزيد من الجرائم من قبلهم. (الحلبي، 1998)

- صعوبة حصر الجرائم المستحدثة ضمن الاحصائيات الرسمية الخاصة بالجرائم على المستوى المحلي لكل دولة.

- التكلفة العالية لهذه الجرائم بعكس الجرائم التقليدية، سواء على المستوى المالي، اوعلى المستوى الأمني الخاص بعمليات المكافحة ومواجهة تلك الجرائم، إضافة إلى الجانب الاقتصادي مما قد يخلق نوعاً من الفوضى في المجتمع.

- الجرائم المستحدثة تشكل خطراً على الأمن العام في المجتمع، فالخوف الناجم عن الجرائم الإرهابية مثلاً اوالاتجار بالأعضاء البشرية يجعل الأفراد في المجتمع في حالة خوف وقلق خصوصاً الأماكن أوالبلدان المستهدفة من قِبل العصابات الإجرامية.

وبناء على ذلك يمكن القول بأن المجتمعات كافة مطالبة بالتصدي لمثل هذه الجرائم، والتقليل من مخاطرها، ولا تقع المسؤولية على عاتق الأجهزة الأمنية فقط، بل على جميع المؤسسات والقطاعات في المجتمع، فالأسرة والمدرسة، والجامعات، والمؤسسات الدينية وإبرازية وغيرها مطالبة بتحمل مسؤولياتها كلُ ضمن اختصاصه للتصدي لهذه الظواهر، لحماية المجتمع والوقاية من المخاطر التي قد تنجم عن هذه الجرائم، فأجهزة الشرطة لا تستطيع لوحدها مواجهة كل هذه الظواهر الإجرامية، لذا يجب على الجميع العمل على خلق المزيد من التعاون بين هذه المؤسسات وأجهزة الشرطة لتصعيب ظروف ارتكاب الجرائم، فالوقاية

والتوعية السليمة تجعل من خلق فرص الجريمة أقل، وتقلل من عدد ضحايا تلك الجرائم ومن آثارها السلبية على المجتمع، كما يتطلب الأمر بناء استراتيجيات خاصة لمواجهة تلك الجرائم واستشراف مستقبلها والتنبؤ بما يمكن أن تكون عليها في المستقبل من أجل الاستعداد لمواجهتها والحد من مخاطرها.

الآثار الناجمة عن الظواهر الجرمية المستحدثة:

من المعروف أن الجرائم المستحدثة لها آثار خطيرة على الأفراد والمجتمعات، وتهدد الاستقرار والأمن فيها، ويمكن حصر بعض الآثار التي تنجم عن الجرائم المستحدثة ومنها: (اليوسف، 2004)

التكلفة الاقتصادية: لا شك بأن الآثار الاقتصادية الناجمة عن الجرائم المستحدثة تكون عالية وقد تفوق التوقعات في بعض الأحيان؛ خصوصاً في الجرائم التي تحدث فيها أضراراً كبيرة في المجتمعات خاصة جرائم الإرهاب وما ينجم عنها من دمار وخراب في البنية التحتية للمجتمع.

- إنعدام الثقة وغياب الأمن: فالجرائم المستحدثة يصعب مواجهتها بصورة مباشرة والقبض على فاعليها، فقد ينتج عنها بعض حالات الانفلات الأمني خاصة في عمليات الإرهاب، والسرقات، والاحتيال والدعارة وغيرها.
- الفوضى الاجتماعية: فقد تؤدي الجرائم المستحدثة إلى الفوضى الاجتماعية، والاضطرابات داخل المجتمع، نظراً لحالة الخوف والرعب من وقوع الجرائم، وكذلك عدم الثقة بقدر المؤسسات في مواجهة تلك العصابات، مثل المؤسسات المالية التي تتعرض لهجمات عديدة من قبل العصابات الإجرامية.

- الخوف من المستقبل: فالتقدم العلمي هدفه خدمة البشرية وتحسين جودة الحياة، إلا أن الاستخدام السيء للتقنيات الحديثة في ارتكاب الجرائم يجعل الناس في حالة قلق من المستقبل خاصة وأن الجرائم والدمار الذي يحصل في المجتمعات أصبح يعتمد بشكل كامل على تقنيات الذكاء الاصطناعي والتكنولوجيا المتطورة.
- إزدياد أنشطة العصابات الإجرامية: تعتمد العصابات الإجرامية على جمع الأموال الطائلة لتنفيذ عملياتها وإدامة أنشطتها الإجرامية، لهذا فوجود المال بين أيدي تلك العصابات يؤثر على اقتصاد الدول وعلى الأمن والاستقرار فيها.
- الفساد القيمي والأخلاقي: تؤدي الجرائم المستحدثة إلى خلق حالة من الفوضى الاجتماعية والأخلاقية في المجتمع وتعمل على تدمير البنى التحتية له، فانتشار الجرائم تخلق حالة من الصراع والخلافات العائلية والأسرية والمجتمعية، مثل انتشار جرائم الدعارة، والاتجار بالبشر والاستغلال والتحرش الجنسي، وغسيل الأموال، وانتشار المخدرات وترويجها. (أبوشامة، 1999)

ويمكن القول بأن الجرائم المستحدثة تركت آثاراً مدمرة على الأفراد والمجتمعات في كافة المجالات، لذلك يجب الوقاية الفردية والجماعية من خلال التنشئة السليمة للجيل القادم وتمكينه من معرفة كل ما يتعلق بهذه التقنيات التي تساعد على ارتكاب الجرائم من أجل الوقاية منها، كذلك يجب العمل على تدريب كافة الكوادر ذات العلاقة على كيفية مواجهة الجرائم المستحدثة ومنع انتشارها في المجتمع.

مراجع الفصل الأول

1. أبوشامة، عباس: التعريف بالظواهر الإجرامية المستحدثة، (1999). الرياض، جامعة نايف، ندوة علمية أقيمت في مركز الدراسات والبحوث.
2. أبوعامر، محمد زكي (1993)، قانون العقوبات القسم العام، الإسكندرية: منشأة المعارف.
3. أقبلي، محمد والعمراني، عابد (2020)، القانون الجنائي الخاص المعمق في شروح المغرب، مكتبة الرشاد للنشر والتوزيع.
4. البشري محمد الأمين (2004) التحقيق في الجرائم المستحدثة، المملكة العربية السعودية، مركز الدراسات والبحوث، جامعة نايف الرياض، ص9.
5. البشري، محمد الأمين، (2007)، الفساد والجريمة المنظمة، السعودية، الرياض، أكاديمية نايف العربية للعلوم الأمنية.
6. بوالماين، نجيب (2008)، الجريمة والمسألة السوسيولوجية- دراسة بأبعادها السوسيوثقافية والقانونية، رسالة دكتوراه غير منشورة، جامعة مونتوري قسنطينة، الجزائر.
7. الجميلي، فتحية عبد الغني (2001). الجريمة والمجتمع ومرتكب الجريمة، الأردن، عمان: المكتبة الوطنية.
8. الحلبي، علي عبد الرزاق: (1998) الجريمة المنظمة والبناء الاجتماعي ورقة قدمت للندوة العلمية السابعة والأربعين الخاصة بالجريمة المنظمة وأساليب مواجهتها في الوطن العربي في مدينة الإسكندرية خلال الفترة 1419/1/22 ه تحت إشراف أكاديمية نايف العربية للعلوم الأمنية.

9. الخليفة عبد اللـه حسن (1999). البناء الاجتماعي والجرائم المستحدثة، بحث منشور ضمن ندوة علمية عقدت في تونس في الفترة من 28- 30 حزيران، وذلك من منشورات جامعة نايف العربية في كتاب الظواهر الإجرامية المستحدثة وسبل مواجهتها، ص 173.

10. الردايده، عبد الكريم (2013). الجرائم المستحدثة واستراتيجية مواجهتها، الأردن، عمان، دار الحامد للتوزيع والنشر.

11. روابح، فريد (2019)، محاضرات في القانون الجنائي العام، الجزائر، سطيف، جامعة محمد لمين دباغين.

12. السراج، عبود (2018)، قانون العقوبات العام، سوريا: منشورات الجامعة الافتراضية

13. السعيد، كامل (2006). شرح الأحكام العامة في قانون العقوبات – الجرائم الواقعة على الأشخاص، الأردن، عمان: دار الثقافة للنشر والتوزيع.

14. الشاذلي، فتوح (2006). أساسيات علم الإجرام والعقاب، لبنان، بيروت: منشورات الحلبي الحقوقية.

15. طالب، أحسن مبارك ونشأت، حسن أكرم. (2001)، الوقاية من الجريمة، دار الطليعة، لبنان، بيروت.

16. عبد المنعم، سليمان (2003). علم الإجرام والجزاء، لبنان، بيروت: منشورات الحلبي الحقوقية.

17. عوده، عبد القادر (1998). التشريع الجنائي الإسلامي مقارناً بالقانون الوضعي، لبنان، بيروت: مؤسسة الرسالة.

18. عياش، أحمد محمود (2003). الانتحار نماذج حية لم تحسم بعد، سوريا، دمشق: دار الفارابي.

19. القصير، فرج (2006)، القانون الجنائي العام، تونس، سوسة، مركز النشر الجامعي.

20. الكساسبة، فهد (2010). وظيفة العقوبة ودورها في الإصلاح والتأهيل، الأردن، عمان: دار وائل للنشر والتوزيع.

21. نجم، محمد صبحي (2006). أُصول علم الإجرام والعقاب، الأردن، عمان: دار الثقافة للنشر والتوزيع.

22. الهراوة، إبراهيم (2015). علم ضحايا الجريمة: من الاهتمام بالجاني إلى الاهتمام بالمجني عليه. المجلة المغربية للقانون الجنائي والعلوم الجنائية: مركز الدراسات والبحوث الإنسانية والاجتماعية، ع2، 167 - 174، ص 167.

23. الوريكات، محمد عبد الله (2009). أصول علمي الإجرام والعقاب، الأردن، عمان: دار وائل للنشر والتوزيع.

24. الوريكات، محمد عبد الله (2010). مبادئ علم الإجرام، الأردن، عمان: دار وائل للنشر والتوزيع، الطبعة الثانية.

25. يسر، أنور علي وآمال عبدا لرحيم (1999). أصول علمي الإجرام والعقاب، مصر، القاهرة: دار النهضة العربية.

26. اليوسف، عبد الله بن عبد العزيز (2004). أساليب تطوير البرامج والمناهج التدريبية لمواجهة الجرائم المستحدثة، الرياض، جامعة نليف عام، ص21.

- **Bernard Marr, (2016) "What Is the Difference Between Deep Learning, Machine Learning and AI?" Forbes (December 8).**

الفصل الثاني

الجريمة المعلوماتية، المجرم الإلكتروني

والتحقيق والأدلة الرقمية

الفصل الثاني

الجريمة المعلوماتية، المجرم الإلكتروني

والتحقيق والأدلة الرقمية

مقدمة

لقد ازداد الاعتماد على التكنولوجيا للقيام بالأعمال التجارية في كل من القطاعين العام والخاص. في عصر المعلومات اليوم، حيث اصبحت التكنولوجيا على غاية من الأهمية لزيادة الإنتاجية وتوفير تكاليف التشغيل الداخلية والخارجية وتعزيز أمان البيانات وتوسيع قدرات الأعمال. المفتاح الرئيسي لتحقيق هذه الفوائد هوتنفيذ التحول الرقمي لجميع جوانب العمل وخاصة عن طريق تخزين البيانات رقميًا كبديل للملفات الورقية . أصبح الأفراد أيضا معتمدين بشكل كبير على التكنولوجيا في حياتهم اليومية، وكل ما يفعله الناس تقريبًا يتضمن التكنولوجيا بطريقة أوبأخرى.

رافق التحول السريع إلى العصر الرقمي زيادة متزايدة في جرائم الإنترنت، حيث يتوقع ان تصل أضرار الجرائم الإلكترونية إلى عشرات التريليونات من الدولار .

المعلومات هي سمة العصر الذي نعيشه حتى إن بعضهم أطلق عليه عصر المعلومات، وتكتسب المعلومات أهميتها من انتشارها ومن تبادلها بين البشر، وما كان لهذا العصر أن يكون عصرا للمعلومات لولا وجود شبكات المعلومات التي كانت الخلايا العصبية التي تولت نقل المعلومات عبر الدول حيث بدأت الثورة المعلوماتية نتيجة اقتران تقنيتي الاتصالات من جهة، والمعلومات وما وصلت إليه من جهة أخرى، فالثورة المعلوماتية هي الطفرة العلمية والتكنولوجية التي نشهدها

اليوم، حتى بات يطلق على هذا العصر عصر المعلومات. وتعد المعلومة أهم ممتلكات الإنسان، اهتم بها، على مر العصور، فجمعها ودونها وسجلها على وسائط متدرجة التطور، بدأت بجدران المعابد والمقابر، ثم انتقلت إلى ورق البردي، وانتهت باختراع الورق الذي تعددت أشكاله، حتى وصل بها المطاف إلى الأقراص الإلكترونية الممغنطة (رستم، 1992)

وتعد الجريمة الإلكترونية من المواضيع الأكثر انتشاراً على المستوى الدولي والإقليمي والمحلي، فلقد أخذت هذه الجريمة، باعتبارها نتاج الاستخدام السلبي للتكنولوجيا وما يتصل بها من تقنيات، حيزاً كبيراً من الاهتمام بهذا الجانب وذلك لجسامة الآثار الناشئة عن هذه الظاهرة الحديثة نوعاً ما وفي جميع مجالات الحياة.

ويواجه المشرع مختلف الجرائم بالتجريم والعقاب كنوع من المكافحة الموضوعية، وفي سبيل ضبط هذه الجرائم والقبض على مرتكبيها يوفر المشرع الإمكانيات البشرية والمادية اللازمة لذلك كنوع من المكافحة الإجرائية، والأمر هنا يبقي عاديا لا يثير أي إشكال ما دمنا بصدد جرائم تقليدية عادية، إلا أنه يختلف إذا ما كنا بصدد جرائم غير عادية جرائم تقع في عالم افتراضي.

فالمصالح التقليدية التي تحميها كل التشريعات والنظم القانونية منذ زمن بعيد بدأت تتعرض إلى اشكال مستحدثة من الاعتداء بواسطة هذه التقنية الحديثة فبعد أن كان الاعتداء على الأموال يتم بواسطة السرقة التقليدية أوالنصب، وكانت الثقة في المحررات الورقية يعتدى عليها بواسطة التزوير، أصبحت هذه الأموال يعتدي عليها عن طريق اختراق الشبكات المعلوماتية واجراء التحويلات الإلكترونية من اقصى مشارق الأرض إلى مغاربها في لحظات معدودة، كما اصبحت تلك الحقوق الثابتة في الاوعية الورقية يتم الاعتداء عليها في اوعيتها الإلكترونية.

والجـرائم الإلكترونيـة هـي كـل سـلوك غـير مشروع يـتم بالتـدخل في العمليـات الإلكترونية أوالمساس بأمن النظم المعلوماتية والمعطيات التي تعالجها، هـذه الجـرائم قلبت موازين التحقيق، فلم يعد الأمر يتعلق بقوة بدنية أومهارات قتالية، وإنما بمدى معرفة المحقق لتقنية المعلومات وإتقانه لمتطلبات إبراز الآلي والاتصال، فهذه المعرفـة هي التي تساهم في القبض على المجرم الإلكتروني.

وفي ظـل تزايـد الجـرائم الإلكترونيـة وتنـوع أنماطهـا وأسـاليبها وقفـت الأجهـزة المختصة بالبحث والتحقيق وعلى رأسها الضبطية القضائية عـاجزة عـن مواكبـة هـذا التطور وملاحقة هذا النوع من الجرائم، وهوالأمر الذي دفع بالعديد مـن الـدول إلى إنشاء أجهزة مختصة تستطيع التعامل مع هذا النوع من الإجرام. "(الدبور، 2017).

المبحث الأول: الجريمة المعلوماتيــة، الجريمــة الإلكترونيــة والمجـرم الإلكـتروني، مبـدأ الأخطـار والتنظـيم التشريعـي للوثـائق الإلكترونيـة، المجـرم الإلكـتروني خصائصـه ومواصفاته:

مفهوم الجريمة المعلوماتية:

يصـعب الاتفـاق عـلى تعريـف موحـد للجريمـة المعلوماتيـة، حيـث اختلفـت الاجتهادات في ذلك اختلافاً كبيرا، يرجع إلى سرعة وتيرة تطور التقنية المعلوماتيـة مـن جهة، وتباين الدور الذي تلعبه هـذه التقنيـة في الجريمـة مـن جهـة أخـرى، فالنظـام المعلوماتي لهذه التقنية يكون محلاً للجريمة تارة، ويكون وسيلة لارتكابها تارة اخـرى، فكلما كان البحث منصباً على الجـرائم التـي ترتكـب ضـد النظـام المعلومـاتي انطلـق التعريـف مـن زاويـة محـل الجريمـة بأنهـا الجريمـة المرتكبـة بالاعتـداء عـلى النظـام المعلوماتي، أما إذا كان البحث منصباً عـلى دراسـة الجـرائم التـي ترتكـب باسـتخدام التقنية المعلوماتية ارتكز التعريف عـلى الوسـيلة وكـان :" كـل أشـكال السـلوك غـير المشروع الذي يرتكب باستخدام الحاسب الآلي (رستم، 1992)

وتجدر الاشارة أيضا إلى أن أهم عوامل صعوبة الاتفاق على تعريف هوأن التقنية المعلوماتية أصبحت تحل محـل العديـد مـن التقنيـات السـابقة كالهـاتف والفـاكس والتلفزيون، فالمسألة لم تقتصر على معالجة البيانات فحسب بل تعـدتها إلى وظـائف عديدة مثل وظيفة النشر والنسخ، وهوما يحتم ضرورة التفرقة بين جـرائم الإنترنـت وشـبكات المعلومـات بـالمعنى الفنـي عـن بقيـة الجـرائم الأخـرى التـي يسـتخدم فيها الإنترنـت أوالحاسـب الآلي كـأداة لارتكابهـا. فيقصـد بجـرائم الإنترنـت وشـبكات المعلومات الـدخول غـير المشروع إلى الشـبكات الخاصـة كالشركـات والبنـوك وغيرهـا

وكذلك الأفراد، والعبث بالبيانات الرقمية التي تحتويها شبكة المعلومات مثل تزييف البيانات أوإتلافها ومحوها، وامتلاك أدوات أوكلمات سرية لتسهيل ارتكاب مثل هذه الجرائم التي تلحق ضرراً بالبيانات والمعلومات ذاتها وكذلك بالنسبة للبرامج والأجهزة التي تحتويها وهي الجرائم التي تلعب فيها التقنية المعلوماتية دوراً رئيسياً في مادياتها أوالسلوك الإجرامي فيها. أما الجرائم التقليدية الأخرى مثل غسيل الأموال، تجارة المخدرات، الإرهاب، الدعارة، الاستخدام غير المشروع للكروت الإلكترونية، ودعارة الأطفال (**Pornography**) وجرائم التجارة الإلكترونية، وكذلك جرائم السب والقذف، هي جرائم تستخدم التقنية المعلوماتية كأداة في ارتكابها دون أن تكون جرائم معلوماتية بالمعنى الفني وإن كان يطلق عليها الجرائم الإلكترونية.

نصل إلى أن الجرائم المعلوماتية لها انواع وأصناف عديدة، وكما أسلفنا القول فإن الجريمة المعلوماتية تتميز بأنها تضم نوعين من الجرائم المستحدثة، الأول انواعاً مسحدثة من الإعتداء على مصالح محمية جنائياً بالنصوص القانونية التقليدية، أي أن في هذه الحالات فإن طرق الاعتداء فقط هي المستحدثة لأنها تتم عن طريق التقنية المعلوماتية بعد أن كانت ترتكب بالسلوك المادي الملموس، أما محل الاعتداء فهي المصالح المحمية اصلا حماية جنائية على مر الأزمان والعصور كالأموال والشرف والاعتبار، أما النوع الثاني فيضم أنواعاً أخرى من الاعتداءات بالطرق المستحدثة على مصالح مستحدثة لم تعرفها القواعد التقليدية كالشبكات المعلوماتية التي تتعرض للإختراق أوالتعطل أوالإغراق (البربري، 2001)

صور الجريمة المعلوماتية:

إذا كانت الجرائم المعلوماتية لها صور متعددة بتعدد دور التقنية المعلوماتية من جهة، وتعدد صور الجرائم التقليدية من جهة أخرى ، فإن ذلك لا يعني تناول هذا الموضوع بالطريقة المدرسية التقليدية التي تتمثل في سرد كل الجرائم التي يتناولها قانون العقوبات، بل يجب التعرض للحالات التي تثير مشكلة في تطبيق النصوص القانونية إما لتعذر المطابقة بينها وبين النصوص التقليدية أوبسبب الفراغ التشريعي لمواجهة هذه الجرائم، ولما كان المجال لا يتسع للحديث عن كل أنواع الجريمة المعلوماتية فقد تخيرنا أكثرها اثارة للمشكلات القانونية وهي جرائم الاعتداء على الحياة الخاصة وجرائم الأموال وجريمة التزوير.

أولاً: جرائم الاعتداء على الحياة الخاصة للأفراد:

المقصود من التطرق لموضوع جرائم الاعتداء على الحياة الخاصة للأشخاص التعرض لتلك الجرائم التي يتعذر علينا مواجهتها بالنصوص التقليدية ، فالاعتداء عليها يتم بواسطة هذه التقنية التي أدت إلى سلب مادية السلوك ومناقشة الحالات التي تثير مشكلة في تطبيق النصوص التقليدية وتكشف مدى الحاجة إلى التصدي التشريعي لهذا النوع من الجرائم وهي جرائم الاعتداء على الحياة الخاصة.

يصعب بداية حصر عناصر الحق في الحياة الخاصة فهي تتكون من عناصر ليست محل اتفاق بين الفقهاء فيمكن القول بأنها تشمل حرمة جسم الإنسان والمسكن والصورة والمحادثات والمراسلات والحياة المهنية (عمر، 2007)

أما علاقة الحياة الخاصة بالتقنية المعلوماتية فقد ظهرت أهميتها بانتشار بنوك المعلومات في الاونه الاخيرة لخدمة اغراض متعددة وتحقيق أهداف المستخدمين في المجالات العلمية والثقافية والعسكرية (قايد، 1994)

هكذا أصبحت الشبكات المعلوماتية مستودعا خطيرا للكثير من اسرار الانسان التي يمكن الوصول اليها بسهولة وسرعة لم تكن متاحة في ظل سائر وسائل الحفظ التقليدية فأصبحت بنوك المعلومات أهم وأخطر عناصر الحياة الخاصة للإنسان في العصر الحديث.

وقد كان ذلك في البداية بالنسبة للمعلومات التي يدلي بها بعض الأشخاص بإرادتهم الخاصة أثناء تعاملاتهم مع المؤسسات العامة والخاصة في البنوك والمؤسسات المالية كمؤسسات الائتمان وشركات التأمين والضمان الاجتماعي وغيرها ، فالبيانات الخاصة بشخصية المستخدم يمكن الوصول اليها عن طريق زيارة بعض المواقع على شبكة المعلومات، لان شبكات الاتصال تعمل من خلال بروتوكولات موحدة تساهم في نقل المعلومات بين الاجهزة وتسمى هذه البروتوكولات الخاصة مثل بروتوكولات **HITP** الذي يمكن عن طريقها الوصول إلى رقم جهاز الحاسب الشخصي ومكانه وبريده الإلكتروني، كما ان هناك بعض المواقع التي يؤدي الاشتراك في خدماتها إلى وضع برنامج على القرص الصلب للحاسب الشخصي وهوما يسمى **cookies** وهدفه جمع معلومات عن المستخدمين. بل ان اخطر ما في استخدام هذه الشبكة يتمثل في ان كل ما يكتبه الشخص من رسائل يحفظ في ارشيف خاص يسمح بالرجوع اليه ولوبعد عشرون عاما . (حجازي، 2007)

ويظن الكثيرون ان الدخول باسم مستعار اوبعنوان بريدي زائف لساحات الحوار ومجموعات المناقشة قد يحميهم ويخفي هويتهم، وفي الحقيقة فإن مزود الخدمة أو**ISP)** **internet service provider)** يمكنه الوصول إلى كل هذه المعلومات بل ويمكنه أيضا معرفه المواقع التي يزورها العميل.

وعلية فإن القوانين المقارنة اهتمت بهذه المسألة واتجهت إلى تبنـي العديـد مـن الضمانات التي يمكن تلخيصها في:

- **مبدأ الأخطار العام :**

وهوأن يعلم الجمهور الهيئات التي تقوم بجمع هذه البيانات وتنوع المعلومـات التي تقوم بتسجيلها . (لويس، 1982)

فيجب أن تكون هناك قيود عـلى انشـاء الأنظمـة المعلوماتيـة المختلفـة لمعالجـة البيانات.

شرعية الحصول على المعلومـة : يجـب أن يـتم الحصـول عـلى المعلومـة بطريقـة تخلومن الغش والاحتيال حيـث تمنـع المـادة 25 مـن القـانون الفـرنسي للمعلوماتيـة تسجيل أي معلومة الا اذا كانت برضاء صاحب الشأن.

التناسب بين المعلومات الشخصية المسجلة والهـدف مـن ذلـك التسـجيل، فعـلى الجهة الراغبة في اقامة أي نظام معلومـاتي ان تحـدد الهـدف مـن إقامتـه . (حجـازي، 2007)

ولقد تضمنت بعض القوانين العربية العديد من النصوص والقواعد التـي تحمـي البيانات الشخصية وتفرد عقوبات على افشـاء هـذا النـوع مـن البيانـات مثـال ذلـك الفصل العاشر من قانون التجارة الآليكترونية المصري الصـادر سـنة 2004 الـذي نـص على حماية سريـة البيانـات المشـفرة واحـترام الحـق في الخصوصـية ، وكـذلك قـانون التجارة الإلكترونية وقانون التجارة والمعاملات الإلكترونيـة في امـارة دبي الصـادر سـنة 2002 وقـانون التجـارة الآليكترونيـة التـونسي الصـادر سـنة 2000 وهومـا يعنـي ان المشرع الليبي تأخر كثيرا في اللحاق بهذا الركب، خاصة بعد ان صدر القـانون العـربي النمـوذجي لجـرائم الكومبيـوتر، والـذي تـم اعـداده مـن قبـل اللجنـة المشـتركة بـين

المكتب التنفيذي لمؤتمر وزراء العدل العرب والمكتب التنفيذي لمؤتمر وزراء الداخلية العرب تحت رعاية جامعة الدول العربية وجرى اقراراه بوصفه منهجا استرشاديا يستعين به المشرع الوطني عند اعداد تشريع في جرائم المعلوماتية، فماهي حدود الحماية الجنائية للحياة الخاص في القانون الجنائي الليبي؟

تتمثل النصوص االجنائية التي صيغت لحماية الحياة الخاصة في تجريم الأفعال التالية:

أول هذه الجرائم هي جريمة انتهاك حرمة المسكن التي نصت عليها المادة 436 ع. وذلك لما للمسكن من أهمية كبرى في نظر المشرع الليبي، لا لأن للمسكن حرمة كبرى فقط لكن لأن المسكن في ثقافة المشرع الذي وضع هذا النص يمثل قلعة حصينة لا يمكن اخاراقها الا بالدخول المادي غير المشروع وأودون رغبة صاحبه .

أما جريمة الاطلاع على الرسائل فقد نصت عليها المادة 244ع التي أن (يعاقب بالحبس مدة لا تقل عن 6 أشهر كل موظف عمومي تابع لمصلحة البريد أوالتلفون أخفى اواوقف رسالة اوأطلع عليها وافشى للغير ما حوته ويراد من الرسالة المكاتبات والمحادثات التليفونية والبرقيات وما إلى ذلك من وسائل الارسال) اما اذا ارتكب الافعال المذكورة اشخاص أخرون فتكون العقوبة الحبس مدة لا تزيد على ستة أشهر اوالغرامة التي لا تتجاوز عشرين جنيها على ان يكون ذلك بناء على شكوى الطرف المتضرر. فإذا كان المشرع الليبي قد توسع في مفهوم الرسالة حيث يمكننا سحب مفهومها في هذا النص على رسائل البريد الإلكتروني الا ان هذه الحماية لا يمكن ان تمتد إلى البيانات المخزنة في أي نظام من نظم المعلومات لأي جه اخرى سواء كانت عامة اوخاصة ، فالحاسب الآلي اليوم لم يعد جهازا للاتصال ومعالجة المعلومات، فقط بل اصبح مستودعا ضخما للمعلومات والبيانات في آن واحد.

نص المشرع كذلك على جريمة اذاعة معلومات تتعلق بإجراء جنائي في المادة 284ع، وهنا الحماية مقتصرة على الإجراءات الجنائية.

أما جريمة افشاء اسرار الوظيفة المنصوص عليها في المادة 236 ع فتتمثل في (كل موظف عمومي يخل بواجبات وظيفته اويسئ استعمالها بأن يفشي معلومات سرية أويسهل بأي طريقة كانت الوصول إلى الإفشاء بها) .و يتضح من هذا النص انه يتضمن شرطا مفترضا يتمثل في ان الجاني في هذه الجريمة موظفا عموميا بالإضافة إلى ان هذه الحماية تقتصر على المعلومات الرسمية ومن ثم تكون هذه الحماية قاصرة على حماية البيانات الاسمية اوالشخصية غير الرسمية والمخزنة في نظم المعلوماتية معينة وهوما نصل معه إلى عدم وجود أي نص يتعلق بحماية المعلومة أوالبيانا الخاصة بصفة عامة بغض النظر عن مصدرها وعن النظام المعلوماتي المخزنة فيه، سواء تم جمعها من قبل الموظف العام ام غيره .

إن التطور التشريعي الوحيد الذي حصل في ليبيا كان بصدور القانون رقم 4 لسنة 1990 بشأن النظام الوطني للمعلومات والتوثيق، الذي يهدف إلى انشاء نظام وطني للمعلومات والتوثيق ليكون دليلا وطنيا للمعلومات والاحصاءات ومتاحا لأجهزة الدولة لتتخذ على ضوء مؤشراتها القرارات السليمة.

نصت المادة 8 منه على الحماية الجنائية للبيانات المخزنة في هذا النظام بتجريم سوء استعمال ، اوحيازة هذه البيانات ، اوالتقصير في التزام تسجيلها ، اوالاخلال بواجب الحفاظ على سريتها ، اواساءة استخدامها ، اوالحصول على البيانات بطريقة غير مشروعة أوحجبها اواتلافها اوتغييرها.

إلا أن هذه الحماية تقتصر على المعلومات المخزنة في هذا النظام الوطني المنصوص عليه في هذا القانون ولا تنطبق على غيره من البيانات، سواء تلك المخزنة

في المؤسسات العامة اوالخاصة، كشركات التأمين والمستشفيات والمصارف اوشركة LTT الليبية وهي الشركة المحتكرة لخدمة التزود بإشتراك الانترنت باعتباره ISP service provider - Internet الوحيد في ليبيا والذي تعج أجهزته الخادمة بالبيانات الخاصة وبالمعلومات الكاملة عن العملاء وملاحتهم داخل الشبكة، والمواقع التي يزورونها بالإضافة إلى أن هذا القانون لم ينص على تجريم اختراق هذا النظام فالمادة 7/8 تنص على الحصول على المعلومة بطريقة التحايل اوالاكراه ولم تنص على الاختراق، الذي كثيرا ما يحدث خطا وبشكل غير متعمد، وهوما يتطلب أن يتم تجريم الاختراق بوصفي العمد والخطأ، إذا ما تعمد المستخدم البقاء في النظام بعد الولوج اليه خطأً، وذلك لان القانون رقم 4 صدر سنه 1990 قبل ان يكون استخدام شبكة الانترنت متاحا للجمهور في ليبيا، ولما كان الاختراق يمثل اخطر صور الجرائم المعلوماتية فإن النص على تجريمه يجب ان يكون صريحاً.

فالقانون رقم 4 عبارة عن قانون يهدف لإنشاء نظام وطني للبيانات ، تتخذ على ضوئها القرارات السليمة في مختلف الأنشطة والمجالات، أي أنه نظام قانوني لحماية مستودعا وطنياً للمعلومات، لكنه لا يكفي لحمايته لوكان متصلا بشبكة الإنترنت.اما القانون العربي النموذجي السابق الإشارة إليه فقد نص في في المواد من 2-4 على تجريم الدخول غير المشروع إلى أي نظام معلوماتي أوإتلاف بياناته أوتحصل على خدماته بطريق التحايل أوانتهك سرية البيانات المخزنة فيه بأي شكل من الأشكال .

تجدر الإشارة أيضا إلى معاهدة بودابست لسنة 2001 التي تهدف إلى توحيد الجهود الدولية لمكافحة جرائم االكومبيوتروالتي تضمنت العديد من التعريفات للأفعال المجرمة تاركة لكل دولة تحديد العقوبة التي تراها مناسبة للفعل .

فنصت المادة 2 منها على تجـريم الـدخول غـير المشروع **illegal access** إلى أي نظام معلوماتي، ونصت المادة 3 منها على أن تجرم الدول الأعضاء كـل اعـتراض لهـذه البيانات باي وسيلة اليكترونية دون وجه حق ، أما المواد 4- وما بعـدها فنصـت عـلى تجريم اي تعديل في البيانات أوتحريفها أوتـدميرها أوتعـديلها أوتغيـير مسـارها، كـما نصت المادة 5 على تجريم التدخل في النظام المعلوماتي والعمليات المنطقيـة ونصـت المادة 6 على إساءة استخدام النظام المعلوماتي بشكل يؤدي إلى افشـاء نظـم الحمايـة الخاصة به دون وجه حق .

هكذا نجد أنه على المشرع الليبي التدخل بالحماية الجنائيـة اللازمـةلأن عنـاصر الحياةالخاصة لم تعد تقتصر عـلى المسـكن والصـورة والمحادثـات الهاتفيـة أوالرسـائل البريدية، فتقنية المعلومات في عصر العولمة قد أفرزت عناصر مستحدثة للخصوصـية يجب أن تشكل مراكز قانونية جديدة، في حاجة ماسة للحماية.

هكذا نجد أن الحق في الحياة الخاصة بعناصره المستحدثة غير مشمول بالحمايـة الجنائية اللازمة، فهل تحظى الأموال بهذا القدر من الحماية الجنائية ؟

ثانياً: جرائم الاعتداء على الأموال:

إذا كان قانون العقوبات الليبي شأنه شأن كل قوانين العقوبات الأخرى قـد جـرم الاعتداء على الأموال في صوره التقليدية كالسرقـة والنصـب وخيانـة الأمانـة واخـتلاس الأموال العامة، فقد كان ذلك في ظل عصر لا يعرف سوى النقـود الورقيـة أوالمعدنيـة ومـا يحـل محلهـا مـن صـكوك أوأوراق ماليـة كالكمبيـالات والسـند الأذني في عصر المصارف التقليدية ذات المقر المحدد مكانيا وقد كان أقصى ما وصلت اليه مـن تقـدم متمثلا في اجراء التحويلات المصرفية بـإجراءات ورقيـة معقـدة ومقابـل رسـوم ماليـة

معينة. فإذا كان الركن المادي للسرقة المتمثل في الاختلاس يمكن ان يطبق على التحويلات المالية غير المشروعة التي تتم عبر المصارف التقليدية فذلك لأن جريمة السرقة من الجرائم ذات القالب الحر لم يحدد المشرع شكل السلوك الإجرامي لها، يمكن أن يتم بأي فعل يؤدي إلى حرمان المجني عليه من المال المنقول وإدخاله في حيازة الجاني، كذلك الحال بالنسب لجريمة النصب حيث يتحقق السلوك الإجرامي لها بالاستيلاء على أموال الآخر بالطرق الاحتيالية، فهل ينطبق ذلك على جرائم السرقة والاحتيال التي ترتكب عن طريق التقنية المعلوماتية ؟

لذا سوف نعرض إلى الوسائل الفنية التي يتم عن طريقها الاختلاس قبل أن نعرض تكييفها القانوني في ظل الفراغ التشريعي في ليبيا.

- **الوسائل الفنية للتحويل الإلكتروني للأموال:**

يتم التحويل غير المشروع للأموال بعدة وسائل يصعب حصرها لسرعة وتيرة التطور في هذا المجال لكن يمكن الاشارة إلى أكثرها انتشاراً.

1. استخدام برامج معده خصيصا لتنفيذ الاختلاس: اشهر هذه الوسائل هوتصميم برامج معينة تهدف إلى اجراء عمليات التحويل الآلي من حساب إلى اخر سواء كان ذلك من المصرف نفسة اومن حساب أخر في مصرف اخر على أن يتم ذلك في وقت معين يحدده مصمم هذا البرنامج، واشهر هذه الوقائع قيام احد العاملين بمركز الحاسبات المتعاقد مع مصرف الكويت التجاري لتطوير أنظمة المعلومات بالاستيلاء على مبالغ طائلة من المصرف بعد أن تمكن من اختيار خمسة حسابات راكدة في خمس فروع محليه للمصرف واعد لها برنامجا تمثلت مهمته في تحويل مبالغ معينة من هذه الحسابات التي حسابات أخرى فتحت

باسمه في الفروع نفسها على أن تتم عملية التحويل أثناء وجوده بالطائرة في طريقة إلى المملكة المتحدة عائدا إلى بلاده بعد انتهاء عقد عمله، ثم فتح حسابات أخرى فور وصوله وطلب من المصرف تحويل هذه المبالغ إلى حساباته الجديدة في بريطانيا . (رستم، 1992)

كما توجد برامج أخرى تقوم بخصم مبالغ ضئيلة من حسابات الفوائد على الودائع المصرفية بإغفال الكسور العشرية بحيث يتحول الفارق مباشرة إلى حساب الجاني لأنها برامج تعتمد على التكرار الآلي لمعالجة معينة ومما يؤدي إلى صعوبة اكتشاف هذه الطريقة رغم ضخامة المبلغ هوان هذه الاستقطاعات تتم على مستوى ألاف الأرصدة في وقت واحد مع ضآلة المبلغ المخصوم من كل حساب على حده بحيث يصعب أن ينتبه اليه العميل. (1996 **David Bai,**)

2. التحويل المباشر للأرصدة: يتم ذلك عن طريق اختراق أنظمة الحاسب وشفرات المرور ، أشهرها قيام احد خبراء الحاسب الآلي في الولايات المتحدة باختزاق النظام المعلوماتي لأحد المصارف وقيامه بتحويل 12 مليون دولار إلى حسابه الخاص في ثلاث دقائق فقط وعادة ما يتم ذلك أيضا عن طريق ادخال معلومات مزيفة وخلق حسابات ومرتبات وهمية وتحويلها إلى حساب الجاني ، ويمكن ان يتم التحويل المباشر أيضا عن طريق التقاط الاشعاعات الصادرة عن الجهاز اذا كان النظام المعلوماتي متصلا بشبكة تعمل عن طريق الاقمار الصناعية فهناك بعض الأنظمة إلى تستخدم طابعات سريعة تصدر اثناء تشغيلها اشعاعات اليكترومغناطيسية ثبت أنه من الممكن اعتراضها والتقاطها اثناء نقل الموجات وحل شفراتها بواسطة جهاز خاص لفك الرموز واعادة بثها مرة أخرى بعد تحويرها. (الشوا، 1994) وهوما نصت عليه اتفاقية بودابست في المادة 5

التلاعب بالبطاقات المالية : لقد ظهرت اولى هذا النوع من الاحتيال بالتقاط الارقام السرية لبطاقات الائتمان وبطاقات الوفاء المختلفة من أجهزة الصرف الآلي للنقود إلى أن ظهرت الصرافة الآلية **Electronic Banking** والنقود المالية **digital Cash** .

أما جرائم الاعتداء على هذه البطاقات فتتمثل في استخدامها من قبل غير صاحب الحق بعد سرقتها أوبعد سرقة الارقام السرية الخاصة بها وهوما يتم عن طريق اختراق بعض المواقع التجارية التي يمكن ان تسجل عليها أرقام هذه البطاقات. وفي هذا النوع من الاعتداءات لا نجد صعوبة في تطبيق نصوص جرائم السرقة والنصب عليها سواء تم ذلك عن طريق سرقة البطاقة نفسها، أوعن طريق سرقة الرقم السري واستخدامه استخدام غير مشروع للتحايل على المؤسسات المالية وصرف هذه المبالغ خاصة أن النموذج التجريمي لجريمة النصب لم يشترط في الوسائل الاحتيالية ان تكون مرتكبة ضد الانسان فيكفي ان ترتكب هذه الوسائل الاحتيالية ضد الآلة ما دامت تؤدي إلى الحصول على نفع غير مشروع اضرارا بالاخر من وهوما نصت عليه المادة 461ع.

جرائم الاعتداء على أجهزة الصرف الآلي للنقود : تثور هذه المشكلة في حالة استخدام الجهاز لصرف ما يتجاوز الرصيد الفعلي اذا تم ذلك بواسطة العميل صاحب البطاقة فالمسألة هنا لا تعدوأن تكون مسألة مديونية بين المؤسسة المالية والعميل ولا يمكن تكييفها بأنها سرقة طبقا للمادة 444ع لان الاستيلاء على المبلغ لم يتم دون رضاء المؤسسة المالية طالما ان هذه الاخيرة تعلم بأن الجهاز غير مرتبط بسقف حساب العميل حتى لا يتجاوزه.

جرائم الاستيلاء على النقود الإلكترونية :يمكن تعريف النقود الإلكترونية **Electronic Cash** بأنها "قيمة نقدية مخزنة على وسيلة إلكترونية مدفوعة مقدماً،

وغير مرتبطة بحساب مصرفي، تحظى بقبول غير من قام بإصدارها، وتستعمل كأداة دفع". وتتمثل أهم عناصرها في أن قيمتها النقدية تشحن على بطاقة بلاستيكية، أوعلى القرص الصلب للحاسب الشخصي للمستهلك، فهي تختلف عن البطاقات الإئتمانية، لأن النقود الإلكترونية يتم دفعها مسبقاً، بالإضافة إلى أنها ليست مرتبطة بحساب العميل، فهي أقرب إلى الصكوك السياحية منها إلى بطاقة الائتمان، أي أنها استحقاق عائم على مؤسسة مالية، يتم بين طرفين هما: العميل والتاجر، دون الحاجة إلى تدخل طرف ثالث، كمصدر هذه النقود مثلاً . (الشافعي، 2004) فهي مجموعة من البروتوكولات والتوقيعات الرقمية التي تتيح للرسالة الإلكترونية أن تحل فعليا محل تبادل العملات النقدية . (الجهني، 2006)، ومن هذه البطاقات ما يعمل عن طريق إدخالها إلى المركز الخاص بالمعاملة المصرفية لدى البائع أوالدائن حيث تم انتقال البيانات الاسمية من البطاقة إلى الجهاز الطرفي للبائع تحول عليه نتائج عمليات البيع والشراء إلى البنك الخاص بالبائع .(حجازي، 2007)

- **التكييف القانوني لهذه الأنماط من السلوك**

ولقد تدخل القانون العربي النموذجي بالنص مع تجريم الصور السابقة والاستيلاء على الأموال فنص في المادة 6 على انه كل من استخدم بطاقة ائتمانية للسحب الإلكتروني من الرصيد خارج حدود رصيده الفعلي أوباستخدام بطاقة مسروقة اوتحصل عليها بايه وسيلة بغير حق أواستخدام أرقامها في السحب اوالشراء وغيرها من العملات المالية مع العلم بذلك يعاقب بالحبس وبالغرامة. وعوما يعني أن هذا النص قاصرا على توفير الحماية لغيرها من البطاقات لتقدير الدولة.

أما اتفاقية بودابست السابق الإشارة اليها فقد نصت المادة 8 منها والخاصة بالتحايل المرتبط بالحاسب**computer related frau** على معاقبة أي شخص

يتسبب باي خسائر مادية للغير عن طريق تعديل أومحوأوإيقاف لأي بيانات مخزنة في أي نظام معوماتي أوعن طريق أي تدخل فيه، وبذلك تتوفر الحماية الجنائية اللازمة للأموال في مواجهة السلوك المرتكب بالحاسب الآلي.

إذا كانت جرائم الأموال المرتكبة بواسطة الحاسب الآلي تواجه فراغا تشريعيا في ليبيا فإن المشكلة الحقيقية في نظرنا بالنسبة لهذه الجرائم لا تتمثل في الفراغ التشريعي بقدر ما هي كامنة في طرق ضبطها وإثباتها، وهوما يرجع إلى افتقاد الاثار التقليدية التي قد تتركها أي جريمة في الجريمة المعلوماتية، فالبيانات يتم إدخالها باشرة في الجهاز دون ان تتوقف على وجود وثائق اومستندات لانه كثيرا ما يكون هناك برامج معدة ومخزنة سلفا على الجهاز ولا يكون عليه سوى ادخال البيانات في الاماكن المعدة لها كما هوالحال بالنسبة للمعاملات المصرفية والمؤسسات التجارية الكبرى ويمكن في هذه الفروض اقتراف جرائم الاختلاس والتزوير فتفقد الجريمة اثارها التقليدية . (حجازي، 2005)

فالجريمة المعلوماتية ترتكب في مسرح خاص هويتمثل في عالم افتراضي مفرغ **cyberspace** وهوما يختلف كليا عن المسرح الذي ترتكب فيه الجرائم في صورتها التقليدية حيث تطبق القواعد العامة لانتداب الخبراء في اقتفاء اثار الجناة، الذين يرتكبون جرائم تتكون من سلوك مادي ملموس وله محل مادي ملموس أيضا، مما لا يتناسب ونوع الخبرة المطلوبة لمعاينة المسرح السيبيري للجريمة المعلوماتية المرتكبة في الفضاء الإلكتروني.

فالخبرة المطلوبة للتحقيق في الجريمة المعلوماتية يجب ان تكون على درجة عالية من الكفاءة العلمية اوالعملية أيضا، وهوما يوجب أن يكون الخبير في الجريمة المعلوماتية ملما بأدق تفاصيل تركيب الحاسب وعمل الشبكات المعلوماتية

والأماكن المحتملة للأدلة كالمواضع التي يمكـن ان تحـتفظ بآثـار الاخـتراق وتوقيتـه، والبرامج المستخدمة في أي عملية تمت اثناء الاختراق، بالإضافة إلى إمكانية نقل الأدلة إلى أوعية أخرى دون تلف.

يجب الإشـارة أيضـا إلى ان ملاحقـة الجـرائم المعلوماتيـة لا يتطلـب رفـع كفـاءة الخبراء فقط بل أنها تحتاج إلى رفع كفاءة مأموري الضـبط القضـائي بصـفة عامـة لان مأمور الضبط القضائي أول شخص يكتشف الجريمة ويتصل بمسرحهـا والمسـئول الأول عن التحفظ على اي اثر يتركه الجاني بعد ارتكابه للجريمة ، مـما يسـتوجب ان يكـون المتعامل الأول مع النظام المعلوماتي على درجة من الكفاءة تسمح لـه بـالتحفظ عـلى هذه الأدلة لأن أي خطأ في التعامل الأولى مع هذه الأجهـزة قـد يـؤدي إلى محـوالأثر أوالأدلة.

أما اتفاقية بودابست السابق الاشارة اليها فقد أشارت في القسم الإجـرائي منهـا في المادة 16 إلى أنه (على الدول الأعضاء العمل على تطبيق أنظمة فنية لحماية البيانات المخزنة مع الزام العاملين في أي نظام معلوماتي بحفظ كـل العمليـات المنطقيـة التـي تجري على الأجهزة لمدة لا تقـل عـلى 90 يومـا)، وهومـا يعنـي ان الاتفاقيـة تشـترط مستوا معيناً للكفاء الفنية في العمل بهذه التقنية، مما يعنـي اننـا نحتـاج إلى برنـامج وطني متكامل لرفع مستوى كفاءة العمل بهذه التقنيـة قبـل الحـديث عـن امكانيـة تطبيق هذه المعاهدة.

ثالثاً: جريمة التزوير:

نصت المادة 341ع على ان يعاقب بالحبس مـدة لاتقـل عـن ثـلاث سـنوات كـل موظف يضع اثناء ممارسة مهامه وثيقـة مـزورة في كليتهـا اوجـزء منهـا اوزور وثيقـة

صحيحة، ما يهمنا في هـذا الصـدد محـل جريمـة التزويـر لان هـذه الاخـيرة مـن مـن الجرائم ذات القالب الحر التي لم يحدد المشرع فيها شـكلا معنيـا للسـلوك الإجرامـي في لكنه حدد محل هـذا السـلوك بالوثيقـة دون أن يعرفهـا اويحـدد مضـمونها تاركـا للفقة والقضاء هذه المهمة.

فالوثيقة هي مجموعة من المعاملات والرمـوز التـي تعـبر تعبـيرا اصـطلاحيا عـن مجموعة مترابطة من الافكار والمعاني الصادرة عن شخص اواشخاص معينـين، وتكمـن القيمة الحقيقية لها ليس في مادتها اوما تحتويه بل تكمن فيما لهذا التعبير من دلالة اجتماعية. (حسني، 1972)

فجوهر جريمة التزوير هوالاخلال بالثقة العامة التي اراد المشرع حمايتها في هذه الوثيقة لما لها من اثار قانونية باعتبارها وسـيلة للإثبـات . (الشـوا، 1994) ولمـا كـان ذلك، فإن قوة الوثيقة في الإثبات هى جوهر الحماية الجنائية لهـا ومـن هنـا ذهبـت بعض الآراء الفقهية إلى أن كل مادة تصلح للإثبات يجوز أن تكون محلا للتزوير مهما كان شـكلها اومسـاحتها ولا اهميـة للـمادة المسـتعملة في الكتابـة يسـتوى ان تكـون مصنوعة من خشب اوجلد.(المرصفاوي، 1991)

فإذا كانت فكرة التوسع في مفهم الوثيقة مطروحة في الفقـة الجنـائي قبـل ظهـور جرائم المعلوماتية فإن هذا التوسع يبدوأكثر الحاحا في ظل الفراغ التشريعي لمواجهـة جرائم التزوير المرتكبة بواسطة الحاسب الآلي، الأن هذا الاتجـاه واجـه نقـداً شـديداً حيث ذهب جانـب مـن الفقـة الفـرنسي قبـل صـدور القـانون رقـم 19 لسـنة 1988 الخاص بالغش المعلوماتي إلى رفض اعتبار التعبير الواقع على يؤيـد هـذا الـرأي قيـاس ذلك على انتفاء التزويـر في التغيـير الـذي يطـرأ عـلى الصـوت المسـجل، والعلـة هـي انعدام عنصر الكتابة، بالإضافة إلى أن النبضات الالكترومغناطيسـية تمثـل جـزءا مـن

ذاكرة الآلة اوبرنامج تشغيلها وهوما يمكن ان يتحقق معه معه الإتلاف اوالتقليد إذا توافرت شروطهما، وقد بدأ الفكر القانوني الحديث يقبل فكرة الوثيقة الآليكترونية استنادا إلى ان المادة التي تصنع منها الوثيقة ليست عنصرا فيها.

إن مجاراة التقديم العلمي والتكنولوجي تتطلب تجاوز المفهوم التقليدي للوثيقة أوحصره في الورق المكتوب. ويمكن لنا في هذه الحالة أن نجد سندا لهذه الفكرة ومنطلقا لها ان المشرع المدني في الاصل رغم أخذه بمبدأ سيادة الدليل الكتابي على غيره من طرق الإثبات إلا أنه أورد عليه بعض الاستثناءات فقبل الإثبات بالبينة فيما كان يجب إثباتها كتابة في حالات حددتها المواد 387 289 391 من القانون المدني الليبي وهي اتفاق الاطراف على الإثبات بالبينة أووجود مانع يحول دون الحصول على الدليل الكتابي فإذا اتفق الاطراف على الإثبات بالبينة يكون على القاضي ان يعتد بها استنادا إلى عدم تعلق القواعد الموضوعية في الإثبات بالنظام العام، مما يمكن القول معه على امكانية اتفاق الأطراف على الإثبات بالوسائل الآليكترونية وهوما يعد ايذانا ببداية عصر الوثائق الإلكترونية.

الاسطوانات الممغنطة تزويراً، استنادا إلى اعتبارين اولهما انتفاء الكتابة ، لان التغيير انصب على نبضات الكترومغناطيسية ، والثاني هوعدم التيقن من صلاحيتها في الإثبات . (الشوا، 1994)

التنظيم التشريعي للوثائق الإلكترونية:

استجابت العديد من دول العالم إلى الاتجاه السابق واعترفت بحجية المستندات الإلكترونية في الإثبات ومن ثم إلى اعتبارها محلا لجريمة التزوير وقد كانت المملكة الأردنية سباقة في ذلك حيث اصدرت قانون الاوراق المالية المؤقت رقم 23 لسنة

1997 الذي نص في المادة 2/24 على ان تعتبر القيود المدونة في سجلات البورصة وحساباتها سواء كانت مدونة يدويا اوالكترونيا اوأي وثائق صادرة عنها دليلا على تداول الاوراق.

أما بالنسبة لتجريم تزوير الوثائق الإلكترونية فقد كان القانون الفرنسي رقم 19 الصادر في يناير 1988 اولى التشريعات التي جرمت تزوير المستندات المعلوماتي فنص في المادة 5/462 على أن (كل من ارتكب افعالا تؤدي إلى تزوير المستندات المعلوماتية ايا كان شكلها باي طريقة تؤدي إلى حدوث ضرر للغير فإنه يعاقب بالسجن من سنه إلى خمس سنوات وغرامه لا تقل عن 20.000 فرنك، ونصت الفقرة السادسة من ذات المادة على معاقبة كل من استخدم بتبصير المستندات المعلوماتية المزورة طبقا للفقرة السابقة، ولم يكتف المشرع الفرنسي بذلك بل انه نص على امكانية ارتكاب جريمة التزوير خطا لان التغيير والتحريف للمعلومات المخزنة خطأً وإن كان غير متصور في المستندات والوثائق التقليدية الا انه كثيرا ما يحدث في المجالات المعلوماتية لان الدخول إلى الأنظمة المعلوماتية لا يحدث دائما بشكل متعمد فمن الممكن ان يحدث بشكل غير معتمد نتيجة الدخول الخاطئ إليه وهوما يجب النص عليه في تجريم التزوير في المستندات المعلوماتية.

أما القانون العربي النموذجي فقد نص على أن كل من غير في البيانات المخزنة في المستندات المعالجة آليا أوالبيانات المخزنة في ذاكرة الحاسب الآلي أوعلى شريط أو اسطوانة ممغنطة أوغيرها من الوسائط يعاقب بـ (   ) وهومتروك لكل دولة على حدة كما نصت المادة 8 منه على تجريم استخدام المستندات المعالجة آليا مع العلم بتزويرها .

تجدر الإشارة إلى أن كل حالات السرقة والاحتيال تتم عن طريق تزوير البيانات لنجد أننا أمام حالة من حالات تعدد الجرائم فالأمثلة التي سبقت الإشارة إليها في الفقرة الخاصة بالسرقة سواء كانت بتصميم برنامج معد خصيصا أو عن طريق إجراء عمليات تحويل غير مشروعة للأرصدة بخلق حسابات دائنة وهمية كلها لا تتم إلا بتزوير في البيانات المخزنة آليا لنجد ان معظم الحالات يتحقق فيها التعدد المعنوي للجرائم خاصة مثل التلاعب الذي يتم في الأرصدة المصرفية لان عمليات التحويل غير المشروعة تتم عن طريق تعديل في البيانات والأسماء اوتعديل في البرامج المعلوماتية المعالجة لهذه البيانات.

فإذا كان السلوك الإجرامي في هذه الحالة متمثلا في تعديل البرامج والبيانات يترتب عليه تحويلات مالية غير مشروعة فإن السلوك اوالفعل يظل واحدا يتحقق به اكثر من نموذج تجريمي في هذه الحالة وهوما يوجب تطبيق احكام التعدد المعنوي والارتباط بين الجرائم.

تجدر الاشارة إلى ان هذا التوسع في تفسير مفهوم الوثيقة لا يغني عن ضرورة تدخل المشرع لمواجهة التزوير المرتكب بالحاسب الآلي على المستندات والوثائق الإلكترونية لان المسالة تحتاج اولا إلى الاعتراف بحجية هذه المستندات الإلكترونية في الإثبات قبل تجريم تحريفها، بالإضافة إلى ان تجريم التعديل في هذه البيانات يجب أن يخضع لعقوبات أشد من عقوبة التزوير التقليدية نظرا لاختلاف حجم الضرر والخسائر الناتجة عن تحريف هذه البيانات وتزويرها.

وقد نصت اتفاقية بودابست في المادة 7 على بتجريم اي تبديل اومحواواخماد لأي بيانات مخزنة في اي نظام معلوماتي يؤدي إلى إنتاج بيانات غير حقيقية - **in authentic data**- لغرض اسعمالها لأغراض قانونية على أنها صحيحة وذلك سواء

كانت فورية القراءة من عدمها **whether or not the data is directly readable and intelligible**

وهوما يقطع الجدل حول قابلية المستند للقراءة بالعين المجردة، واعتبار المستند الآليكتروني وثيقة قابلة للقراءة، مشمولة بالحماية الجنائية.

يتضح لنا أن الجريمة المعلوماتية تثير مشكلات عديدة في تطبيق النصوص القانونية الحالية، فإن وجد النص القانوني وأمكن اعمال المطابقة بينه وبين السلوك المرتكب لا نجد العقوبة تتناسب وحجم الخسائر الناتجة عن ارتكاب مثل هذه الجريمة ، واذا امكن اعمال المطابقة وكانت العقوبة رادعة فإننا نواجه عقبة كبيرة في عمليات ضبط هذه الجرائم وإثباتها لان القواعد التقليدية للإثبات وضعت لتواجه سلوكا ماديا يحدث في العالم الفيزيائي **physical world**، ولا تتناسب لإثبات جريمة مرتكبة في عالم اليكتروني أوفضاء سيبراني افتراضي غير ملموس يتكون من ذبذبات والموجات غير المرئية. وهوما يحتم ضرورة التدخل التشريعي لتنظيم هذه المسألة عنطريق الاعتراف لقوة المستندات الآليكتروني في الإثبات ، واعتبارها من قبيل الوثائق قبل النص على تجريم تزويرها أوالتعديل فيها وتحريفها حسب الأحوال.

مفهوم الجرائم الإلكترونية :

تعتبر الجرائم الإلكترونية هي النوع الشائع من الجرائم، إذ إنها تتمتع بالكثير من المميزات للمجرمين تدفعهم إلى ارتكابها، وقد تكون هذه الدوافع ذات طبيعة ربحية بحيث يسعى الجاني من ورائها إلى الحصول على الأموال، أويكون هدف الجاني هوالرغبة في إثبات الذات وتحقيق انتصار على تقنية النظم المعلوماتية (البقمي، 2008)، كما يُمكن أن يكون الدافع لارتكاب الجريمة تعرض الشخص للتهديد

والضغط من الآخرين في مجالات الأعمال التجارية والأخرى الخاصة بالتجسس والمنافسة، أوسعي بعض الموظفين إلى الانتقام من المنشآت، وقد يكون الهدف تهديد الشخص وابتزازه لحمله على القيام بفعل أوالامتناع عنه، ولوكان القيام بهذا الفعل أوالامتناع عنه مشروعين (الملط، 2005) وقد يكون الدافع ذا طبيعة سياسية، إذ تعد الدوافع السياسية من أبرز المحاولات الدولية لاختراق شبكات حكومية في مختلف دول العالم، كما إن الأفراد قد يتمكنون من إختراق الأجهزة الأمنية الحكومية، كذلك أصبحت شبكة الإنترنت مجالاً خصباً لنشر أفكار العديد من الأفراد والمجموعات ووسيلة للترويج لأخبار وأمور أخرى قد تحمل في ثناياها مساساً بأمن الدولة أوبنظام الحكم أوقدحاً في رموز دولية أوسياسية والإساءة لها بالذم والتشهير(البقمي ، 2008)، كما إمتدت الجريمة الإلكترونية لتشمل صور الجريمة المنظمة، حيث ظهر الإرهاب الإلكتروني على الشبكة، وأخذت الجماعات الإرهابية مواقع لها على الانترنت، تمارس أعمالها من خلالها، كالتحريض على القتل، بالإضافة إلى تعليم صنع المتفجرات والقنابل، علاوة على نشر أفكارها الإرهابية، وأصبحت تقوم بشن عملياتها الإرهابية عبر الانترنت من خلال التلاعب بنظم وبيانات أنظمة خاصة.

لقد وردت مجموعة من التعريفات لهذا القسم من الجرائم، فيرى جانب من الفقه الألماني أنها (كل أشكال السلوك غير المشروع أوالضار بالمجتمع الذي يرتكب باستخدام الحاسب الآلي) (إبراهيم، 2008) ويختصر جانب من الفقه الجنائي جرائم الكمبيوتر بأنها (الاستخدام غير المشروع للحاسبات والتي تتخذ صورة فيروس يهدف إلى تدمير الثروة المعلوماتية) (حجازي، 2006) يتضح من التعريفات التي ذكرناها إنها قد امتازت بالتعدد والاختلاف ضيقاً واتساعا تبعاً

للمعايير والمنطلقات المستندة إليها، فمنها ما اعتمد أصحابها على معيار الوسيلة المستخدمة في ارتكاب الجريمة، وآخرون اعتمدوا معيار موضوع الجريمة ذاتها، ومنهم من اعتمد معايير مختلطة جمعت بين المعيارين السابقين.

ولهذه الجرائم خصائص تميزها وتنفرد بها نوردها بالنقاط الآتية:

1) إن جرائم الحاسوب ترتكب بعضها داخل أجهزة الحاسوب الشخصية في أي مكان حتى في غرف النوم أوداخل الأجهزة الرئيسية الكبيرة المحفوظة في أماكن مجهزة تجهيزاً آمناً.

2) تتميز جرائم الحاسوب بوقت ارتكابها السريع للغاية، لهذا يجب أن يوضع في الاعتبار هذا العنصر الجوهري عند التخطيط لمواجهتها، وذلك نظراً لسرعة تنفيذ اجهزة الحاسوب الفائقة للتعليمات الصادرة إليها وفقاً للمعايير الزمنية للحاسوب.

3) كما تتميز جرائم الحاسوب بأن الحواجز الجغرافية والمكانية لا تُمثل عوائق طبيعية أمام إرتكابها، فمثلاً سرقة الأرصدة النقدية من البنوك باستخدام الحاسوب لا تُواجه العوائق المادية ككسر الأبواب واستخدام السلاح، وإنما يُمكن الدخول غير المشروع على شبكة معلومات البنك وإجراءات تحويلات غير مشروعة لأرصدة مالية ضخمة لحسابات الجاني أوالجناة في نفس البنك أوفي بنوك أخرى، إذ إن أغلبية المؤسسات قد استغنت عن القيود والسجلات المادية بأخرى أكثر حداثة متمثلة بالمستندات الإلكترونية والبصرية الموجودة بأنظمة الحاسوب. (الحيدي، 2012)

ميزات الجريمة الإلكترونية :

تتميز الجرائم الإلكترونية عن الجرائم التقليدية بما يلي:

- بيئة الجريمة الإلكترونية هي بيئة رقمية معلوماتية قوامها البرامج المعلوماتية الحاسوبية واجهزة الحاسب الآلي ومعداته اي مكوناته المادية والبرمجية.
- المجرم في الجرائم الإلكترونية ذوطبيعة خاصة وامكانيات خاصة .
- يغلب على دليل الجرائم الإلكترونية الطبيعة الرقمية لا الطبيعة المادية.
- يستعصي إثبات الجرائم الإلكترونية بالطرق التقليدية فهي تحتاج لإثباتها إلى طرق مستحدثة.
- الجرائم الإلكترونية لا يحدها مكان ولا يحتاج مرتكبها في الغالب إلى وقت طويل.
- الأضرار والخسائر الناتجة عن الجرائم الإلكترونية غالبا فادحة وكبيرة جدا .

إثبات الجريمة الإلكترونية :

إن الجرائم الإلكترونية عادةً ما يتم اكتشافها بالمصادفة، بل وبعد وقت طويل من ارتكابها، فضلاً عن الجرائم التي لم تُكتشف هي أكثر بكثير من تلك التي كُشف الستار عنها، فالرقم المظلم بين حقيقة عدد هذه الجرائم المرتكبة والعدد الذي تم اكتشافه هورقم خطير، وبعبارة أخرى فإن الفجوة بين عدد هذه الجرائم الحقيقي وما تم اكتشافه فجوة كبيرة، وهذا يرجع إلى عدة معطيات تدور حول واقع الجريمة الإلكترونية، وهذا ما سنتولى توضيحه.

معوقات إثبات الجريمة الإلكترونية:

تتمحور هذه المعوقات حول كل متعلقات هذه الجريمة، فمنها ما هومتصل بالجريمة ذاتها والجهات المتضررة، ومنها ما هومتعلق بالجهات التحقيقية والواقع التشريعي الخاص بهذا النوع من الجرائم، وهذا ما سنأتي على بيانه في الآتي:

- المعوقات المتعلقة بالجريمة: هنـاك أمـور تُعيـق سـلطات التحقيـق أثنـاء ممارسـتها لإجراءات التحقيق، وتتمثل هذه الأمور بما يأتي:

1. اختفاء آثار الجريمة وغياب الدليل المرئي الممكن بالقراءة فهمه، إذ إن مرتكبي هذا النوع من الجرائم نادراً ما يتركون آثـاراً ماديـة ملموسـة يمكـن أن تُشـكل طـرف خيط يقود إليهم بفضل مهاراتهم في استخدام هذه التقنيات وبرامجها.
2. صعوبة الوصول إلى الدليل لإحاطته بوسائل الحماية الفنية كاستخدام كلمات السر حول مواقعهم تمنع الوصول إليها أوتشفيرها لإعاقة المحاولات الرامية إلى الوصول إليها والاطلاع على محتواها أواستنساخها.
3. سهولة محوالدليل أوتدميره في زمن قصـير، فالجـاني يُمكنـه محوالأدلـة التـي تكـون قائمة ضده أوتدميرها في زمن قصير جداً، بحيث يصعب على الجهـات التحقيقيـة كشف الجريمة إذا علمت بها.
4. الضخامة البالغة لحجم المعلومات والبيانات المتعين فحصها وامكانية خروجها عن نطاق اقليم الدولة. (الحلبي، 2011)
5. لا يستخدم هؤلاء الجناة في دخولهم شبكة الانترنت أجهـزتهم الخاصـة في أغلـب الأحيان، وإنما يلجئون إلى مقاهي الانترنت المنتشرة حالياً في معظم المدن والأحياء التـي لا تتقيـد بـأي ضـوابط أوأنظمـة أمنيـة يُمكـن مـن خلالهـا التعـرف عـلى مستخدمي أجهزة الحاسب الآلي المتعاقبين في حالة اكتشاف أفعال غـير مشروعـة مصدرها هذه الأجهزة.
6. أغلب البيانات والمعلومات التي يتم تداولها عـبر الحاسـب الآلي وشـبكة الانترنـت هي عبارة عـن رمـوز مخزنـة عـلى وسـائط ممغنطـة لا يُمكـن الوصـول إليهـا إلا

بواسطة الحاسب الآلي ومن قبل أشخاص قادرين على التعامل مع هـذه الأجهـزة ونظمها. (إبراهيم ، 2008)

المعوقات المتعلقة بالجهات المتضررة من الجريمة :

تتمثل المعوقات المتعلقة بالجهات المتضررة بعدة جوانب نلخصها بما يأتي:

1 .عدم ادراك خطورة الجرائم المعلوماتية من قبل المسؤولين بالمؤسسات، وهذا يرجع إلى اغفال جانب التوعيـة لإرشـاد المسـتخدمين إلى خطورتهـا، وبـالنظر إلى بعـض المؤسسات نجد أنها أسست نظم معلوماتها على تطبيقات خاصة من التقنية على أساس إنها تقدم لعملائها خدمات أسرع بدون عوائق ويكون ذلك عـلى الجانـب الأمني.

2.) الحفاظ على سمعة بعض المؤسسات والأفراد، حيث يكـون الإحجـام عـن الابـلاغ عن هذا النوع من الجرائم بسبب عدم رغبة الجهات المتضررة في الظهـور بمظهـر مشين أمام الآخـرين، لأن تلـك الجـرائم ارتكبـت ضـدها، مـما قـد يـترك انطباعـاً باهمالها أوقلة خبرتها أوعدم وعيها الأمني، ولم تتخذ الاحتياطات اللازمـة لحمايـة معلوماتها.

3. تعد التقنية المستخدمة في نظم المعلومات مجال استثمار، ولذا تتسـابق الشركـات في تبسيط الاجـراءات وتسـهيل اسـتخدام الـبرامج والاجهـزة وملحقاتهـا، وزيـادة المنتجات واقتصار تركيزها على تقديم الخدمة وعدم التركيز على الجانب الأمنـي، على سبيل المثال مستخدموشبكة الانترنت عبر مزودي الخدمة وبطاقات الانترنت المدفوعة ليسوا مطالبين بتحديد هويتهم عند الاشتراك في خدمة الانترنـت، أي ان مزود الخدمة لا يعرف هوية مستخدم الخدمة (الحلبي ، 2011)

4 . خشية بعض الجهات المتضررة من الحرمان من الخدمة، اذ ان الافصاح عن التعرض لجريمة معلوماتية من شانه حرمان شخص من خدمات معينة تتعلق بالنظام المعلوماتي، فقد يحرم الموظف في الجهة من خدمات معينة على الانترنت اوقد يحرم من خدمات الانترنت عموماً، حيث يتعرض لجريمة معلوماتية ناتجة عن الاختراق اوزيارته لأماكن غير مأمونة اوغير مسموح بزيارتها، وقد يكون سبب عدم الابلاغ عن الجريمة عدم معرفة الضحية بوجود جريمة اصلاً، وعدم القناعة انها ممكن ان تحدث في مؤسسته (إبراهيم، 2010)

المعوقات المتعلقة بالجهات التحقيقية:

هناك معوقات للتحقيق في جرائم الحاسوب والانترنت تتعلق بالسلطات القائمة بالتحقيق وترجع لعدة اسباب، والاسباب سوف نذكرها كما يلي:

1 . بعض هذه المعوقات ترجع إلى شخصية المحقق، مثل التهيب من استخدام جهاز الكمبيوتر والتهيب من استخدام الانترنت، بالإضافة إلى عدم الاهتمام بمتابعة المستجدات في مجال الجرائم الإلكترونية، بينما في المقابل نجد أن مرتكبي هذه الجرائم يتابعون كل جديد ويعملون على تطوير سبل اخفاء أدلة جرائمهم، فضلاً عن ذلك إن للعاملين في مجال الكمبيوتر مصطلحات علمية خاصة اصبحت تشكل الطابع المميز لمحادثاتهم وأساليب التفاهم معهم، وليس هذا فحسب بل اختصر العاملون في هذا المجال تلك المصطلحات والعبارات بالحروف اللاتينية الأولى لتكون لديهم لغة غريبة تعرف بلغة المختصرات وهي لغة جديدة ومتطورة.

2 . وكذلك من اهم معوقات التحقيق تلك المتعلقة بأساليب المكافحة، مثل عدم توفر الاجهزة والبرامج المناسبة للتحقيق وعدم التنسيق بين المحققين في هيئات التحقيق والعاملين في مجال المعلومات والأنظمة الإلكترونية والحاسوب.

لكل ما ذكرناه انفاً تبدوالحاجة ملحة إلى انشاء وحدة متخصصة للتحقيق في الجرائم الإلكترونية تتكون من محققين وطاقم من ذوي الاختصاص في مجال تقنية المعلومات (الحلبي، 2011)

المعوقات التشريعية:

أولاً: على الصعيد الوطني:

يتصدى قانون العقوبات للظواهر الإجرامية فيُحدد الافعال الجرمية ويضع العقوبات الرادعة لكل منها، وغايته انزال العقاب بالمجرمين وحماية المجتمع من شرورهم وردع غيرهم عن الاقتداء بهم، وهذا يُمثل الشق الأول من المعادلة التشريعية الجزائية، أما الشق الثاني فيتمثل في قانون أصول المحاكمات الجزائية الذي يحدد القواعد الاجرائية والضمانات التي ينبغي أن تسير على هديها الجهات المعنية بإنفاذ القانون في مراحلها المختلفة بدءاً بمرحلة الاستدلال وانتهاءا بالمحاكمة، فالقانونان إذن يُكملان بعضهما.

وكما هوالحال في المعوقات المرتبطة بالجريمة ذاتها أوالجهات المتضررة من الجريمة، كذلك تبرز ذات المشكلة بالنسبة للنصوص المتعلقة بهذه الجرائم، بمعنى آخر هل إن إبقاء الحال كما هوعليه في النصوص التقليدية يكفي لتغطية كل ماهوحديث يفرزه لنا التطور المتسارع، أم إن هناك حاجة لوضع نصوص وقواعد جديدة لتدارك النواقص؟

فبالنسبة لمحور بحثنا برزت لنا بعض الأمور نذكر من ذلك على سبيل المثال، إن المعلومات التي تُشكل عصب الجرائم الإلكترونية إذا وقعت عليها جريمة السرقة، فالمشكلة هنا إن أحد أركان جريمة السرقة هووقوعها على مال منقول لغير الجاني عمداً، فهل إن وصف المنقول ينطبق على المعلومات (مادة الجريمة الإلكترونية) وذلك على اعتبار إن جرائم الأموال تتحقق بخروج المال من حيازة المجني عليه إلى حيازة الجاني، بينما جريمة الأنترنت لا يُشترط في تحققها خروج المعلومات من حيازة المجني عليه وإنما تتحقق الجريمة حتى ولوبقيت المعلومات في حيازة المجني عليه كاستنساخ المعلومات والاستفادة منها لاحقاً.

مثال آخر: إن مفهوم الجريمة المشهودة كما أوضحه المشرع في أصول المحاكمات الجزائية قائمة على معطيات مادية وحسية لا ينسجم مع طبيعة الجريمة الإلكترونية التي عادة لا يظهر منها أية إشارات أومعطيات مادية أوحسية (الحيدري ، 2012)

ثانياً: على الصعيد الدولي:

تُعد جرائم تقنية المعلومات من أكثر الجرائم التي تُثير مشاكل تتعلق بالإختصاص على المستوى الدولي، وذلك بسبب الطبيعة الخاصة لهذا النوع من الجرائم التي تمتاز بقدرتها على التحرك في مجال فضائي واسع لا توقفه حدود الدول وسيادتها الاقليمية، حيث يُمكن لجريمة تقنية المعلومات أن تقع في مكان وتُنتج آثارها في مكان أوأماكن أخرى خارج الدول، وهذا الأمر يدعوإلى التعاون بين الدول من خلال الإتفاق على معايير محدودة، وإن من أبرز المعوقات التي تُواجه الدول لتنظيم موضوع الجرائم الإلكترونية هوتفاوت الدول في تحديد مفهوم الجرائم الإلكترونية وأساليب التعامل معها، وهذا راجع إلى ان كل دولة تعمل على تنظيم موضوع التقنيات الإلكترونية ضمن حدود قيمها السياسية والقانونية والأخلاقية والثقافية.

تعمل عدد من المنظمات الدولية باستمرار لمواكبة التطورات في شأن أمن الفضاء الإلكتروني، وقد أسست مجموعات عمل لوضع استراتيجيات لمكافحة الجرائم الإلكترونية، وأبرز هذه المجموعات والمنظمات الدولية التي عملت في موضوع الجرائم الإلكترونية هوالاتحاد الدولي للاتصالات، ويُمثل هذا الاتحاد الذي يضم اكثر من (192) دولة وأكثر من (700) شركة من القطاع الخاص والمؤسسات والاكاديمية منبراً إستراتيجياً للتعاون بين أعضائه باعتباره وكالة متخصصة داخل الأمم المتحدة، ويعمل الاتحاد على مساعدة الحكومات والصناعات التي تعتمد على تكنولوجيا المعلومات والبنية التحتية للاتصالات، وقد وضع الاتحاد الدولي للاتصالات مخططاً لتعزيز الأمن الإلكتروني العالمي يتكون من سبعة أهداف رئيسة وهذه الأهداف هي:

- وضع أستراتيجيات لتطوير نموذج التشريعات الإلكترونية يكون قابلا للتطبيق محلياً وعالمياً بالتوازي مع التدابير القانونية والوطنية والدولية المعتمدة.
- وضع استراتيجيات لتهيئة الارضية الوطنية والاقليمية المناسبة لوضع الهيكليات التنظيمية والسياسات المتعلقة بالجرائم الإلكترونية.
- وضع استراتيجيات لتحديد الحد الادنى المقبول عالميا في موضوع معايير الأمن ونظم تطبيقات البرامج والأنظمة.
- وضع استراتيجيات لوضع آلية عالمية للمراقبة والإنذار والرد المبكر مع ضمان قيام التنسيق عبر الحدود.
- وضع استراتيجيات لإنشاء نظام هوية رقمي عالمي وتطبيقه، وتحديد الهيكليات التنظيمية اللازمة لضمان الاعتراف بالوثائق الرقمية للأفراد عبر الحدود الجغرافية.

- تطوير استراتيجية عالمية لتسهيل بناء القدرات البشرية والمؤسسية لتعزيز المعرفة والدراية في مختلف القطاعات وفي المجالات المعلوماتية جميعها.
- تقديم المشورة بشان امكانية اعتماد إطار استراتيجي عالمي لأصحاب المصلحة من اجل التعاون الدولي والحوار والتعاون والتنسيق في جميع المجالات التي سبق ذكرها (www.groups.google.com)

إجراءات الإثبات:

إن المحققين يُواجهون العديد من الصعوبات عند ممارسة وظائفهم في إثبات الجرائم الإلكترونية وهوما يتطلب مجهوداً إضافياً وتدريباً وتعاوناً من الجهات ذات العلاقة لإثبات هذا النوع من الجرائم.

التحري وجمع الأدلة في الجرائم الإلكترونية:

التحليل الجنائى الرقمي: (المعروف أيضا باسم الطب الشرعي الرقم) هوعملية التحقيق في الجرائم المرتكبة باستخدام أي نوع من أجهزة الحوسبة (مثل أجهزة الكمبيوتر والخوادم وأجهزة الكمبيوتر المحمولة والهواتف المحمولة، والأجهزة اللوحية والكاميرا الرقمية وأجهزة الشبكات وأجهزة إنترنت الأشياء (**IoT**) أوأي نوع من أجهزة تخزين البيانات).

التحليل الجنائى الرقمي مسؤول أيضا عن فحص الهجمات التي تنشأ من الفضاء الإلكتروني مثل برامج الفدية والتصيد وهجمات أوامر **SQL** وهجمات رفض الخدمة الموزعة (**DDoS**) وخرق البيانات وأي نوع من الهجمات الإلكترونية التي تسبب خسائر مالية أوسمعة. الهدف النهائي للتحقيق الجنائي الرقمي هوالحفاظ على الأدلة الرقمية وتحديدها والحصول عليها وتوثيقها لاستخدامها في المحاكم.

أهمية استخدام التحليل الجنائي الرقمي:

يتم استخدام التحليل الجنائي الرقمي للتحقيق في أي جريمة تنطوي على استخدام الأجهزة الإلكترونية، سواء تم استخدام هذه الأجهزة لارتكاب جريمة أوكهدف لها. يصبح امتلاك القدرة على التحاليل الجنائية الرقمية أمرًا مهمًا جدًا للمنظمات الحديثة للتحقيق في انتهاكات السياسة الداخلية والهجمات الخارجية ضد أنظمتها المحوسبة .

عادةً ما تبقى الجريمة مستترة حتى يصل خبرها إلى السلطات المختصة، هذا الوضع ينطبق على الجرائم كافة دون استثناء، لكنه يتجلى وضوحاً بالنسبة لجرائم تقنية المعلومات نظراً لطبيعتها، حيث يصعب على الأشخاص العاديين الإبلاغ عنها لما تتطلبه من مهارات فنية غير متوافرة سوى لفئات مهنية أوتخصصية في مجال الحاسب الآلي ونظم تقنية المعلومات، وفي الأحوال جميعها فإن أي إخبار عن جريمة سواء كان فاعلها مجهولاً أم معلوماً ينبغي أن يتضمن على الأقل معلومات أولية عن الجريمة مثل تحديد محل الجريمة ومكان وقوعها ونوعها، إذ تُعد هذه العناصر مهمة وضرورية لمساعدة رجال الضبط القضائي في أي إخبار متعلق بجرائم تقنية المعلومات، بحيث تُمكنهم من تحديد معالم الجريمة ووضع خطة للتعامل معها من الناحيتين الفنية والقانونية.

هذا ويتم الكشف عن الجرائم الإلكترونية بوضع برمجيات حاسوبية معينة خصوصاً فيما يخص جرائم القرصنة أونشر المواد الإباحية.

إن استحداث الأدوات البرمجية الحاسوبية التي من خلالها يُمكن التعرف على الأنماط الإجرامية تعد مسألة لا غنى عنها في كشف الجريمة بالنظر لضخامة حجم المعلومات المتوافرة في شبكة الانترنت، وهناك وسيلتان لأعضاء الضبط القضائي

لغرض الحصول على البيانات المتعلقة بارتكاب الجريمة من نظام حاسوب، وهما تستندان إلى معايير تقنية وقانونية، وتتمثل بما يأتي:

1. يتم الحصول على المعلومات من الموقع نفسه الذي تم من خلاله ارتكاب الجريمة بعد أن يتم إكتشافه باستخدام البرمجيات الحديثة.
2. يتم الحصول على المعلومات عن طريق اعتراض أورصد البيانات المنقولة من الموقع أوإليه أوفي إطاره (الحيدري ، 2012) أما إذا كانت الجريمة مشهودة كما لوتم ضبط الفاعل وهويستخدم موقع الانترنت لارتكاب إحدى الجرائم، فعلى عضوالضبط القضائي إخبار قاضي التحقيق والادعاء العام بوقوع الجريمة وينتقل فوراً إلى محل الحادثة ويسأل المتهم عن التهمة المُسندة إليه ويضبط كل ما يظهر إنه استعمل في ارتكاب الجريمة من مخرجات ورقية وشرائط وأقراص ممغنطة وغيرها من الأشياء التي يُعتقد إن لها صلة بالجريمة ويسمع أقوال من يُمكن الحصول منه على معلومات وأيضاحات في شأن الحادثة ومرتكبها ويُنظم محضراً بذلك . وبشكل عام على المكلفين بمعاينة مسرح الجريمة اتباع جملة من الارشادات التي قد تسهم بإزالة الغموض المحيط بملابسات ارتكاب الجريمة وهي: (إبراهيم ، 2010)

- التحفظ على الأجهزة وملحقاتها والمستندات الموجودة من مخرجات ورقية وشرائط وأقراص ممغنطة وغيرها من الاشياء التي يعتقد ان لها صلة بالجريمة.
- إثبات الطريقة التي تم بواسطتها اعداد النظام والعمليات الإلكترونية، وخاصة ما تحتويه السجلات الإلكترونية التي تزود بها شبكات المعلومات لمعرفة موقع الاتصال ونوع الجهاز الذي تم عن طريقه الدخول إلى النظام.

- عدم نقل أي مادة متحفظ عليها من مسرح الجريمة قبل التأكد من خلوالمحيط الخارجي بموقع الحاسب الآلي من أي مجالات لقوة مغناطيسية يُمكن أن تسبب في محوالبيانات المسجلة عليها.
- إثبات حالة التوصيلات والكابلات المتصلة بمكونات النظام كله، وذلك لا جراء مقارنة لدى عرض الأمر على القضاء.

مواصفات المجرم الإلكتروني:

فيما يلي عرضا لبعض الصفات العديدة للمجرم الإلكتروني والتي في الغالب تميزه عن غيره من المجرمين العاديين:

أولا: المجرم الإلكتروني، مجرم متخصص

تبين في عديد من القضايا أن عددا من المجرمين لا يرتكبون سوى جرائم الكمبيوتر أي أنهم يتخصصون في هذا النوع من الجرائم، دون أن يكون لهم أي صلة بأي نوع من الجرائم التقليدية الأخرى، مما يعكس أن المجرم الذي يرتكب الجرائم الإلكترونية هومجرم في الغالب متخصص في هذا النوع من الإجرام.

ثانيا: المجرم الإلكتروني، مجرم عائد إلى الإجرام

يعود كثير من مجرمي المعلومات إلى ارتكاب جرائم أخرى في مجال الكمبيوتر انطلاقا من الرغبة في سد الثغرات التي أدت إلى التعرف عليهم وأدت إلى تقديمهم إلى المحاكمة في المرة السابقة، ويودى ذلك إلى العودة إلى الإجرام، وقد ينتهي بهم الأمر كذلك في المرة التالية إلى تقديمهم إلى المحاكمة.

ثالثا: المجرم الإلكتروني، مجرم محترف

يتمتع المجرم الإلكتروني باحترافية كبيرة في تنفيذ جرائمه، حيث أنه يرتكب هذه الجرائم عن طريق الكمبيوتر الأمر يقتضى الكثير من الدقة والتخصص والاحترافية في هذا المجال للتوصل إلى التغلب على العقبات التي أوجدها المتخصصون لحماية أنظمة الكمبيوتر كما في حالة البنوك والمؤسسات العسكرية.

رابعا: المجرم الإلكتروني، مجرم غير عنيف

المجرم الإلكتروني من المجرمين الذين لا يلجأون إلى العنف بتاتا في تنفيذ جرائمهم وذلك لأنه ينتمي إلى إجرام - الحيلة - فهولا يلجا إلى العنف في ارتكاب جرائمه، وهذا النوع من الجرائم لا يستلزم أي قدرا من العناء للقيام به.

فضلا عما تقدم، فالمجرم الإلكتروني مجرم ذكى، ويتمتع بالتكيف الاجتماعي، أي لا يناصب أحد العداء وأيضا يتمتع بالمهارة والمعرفة وأحيانا كثيرة على درجة عالية من الثقافة (مصطفى، 1994)

خصائص المجرم الالكتر وني:

يتميز المجرم الإلكتروني كذلك بمجموعة من الخصائص التي تميزه بصفة عامة عن غيرة من المجرمين، وهى:

أولا: المهارة

يتطلب تنفيذ الجريمة الإلكترونية قدرا من المهارة يتمتع بها الفاعل، والتي قد يكتسبها عن طريق الدراسة المتخصصة في هذا المجال، أوعن طريق الخبرة المكتسبة في مجال التكنولوجي، أوبمجرد التفاعل الاجتماعي مع الآخرين، وهذه ليست قاعدة في أن يكون المجرم الإلكتروني على هذا القدر من العلم ، وهذا ما اثبته

الواقع العملي أن جانب من انجح مجرمي المعلوماتية، لم يتلقوا المهارة اللازمة لارتكاب هذا النوع من الإجرام.

ثانيا: المعرفة

تميز المعرفة مجرمي المعلوماتية، حيث يستطيع المجرم الإلكتروني أن يكون تصورا كاملا لجريمته، ويرجع ذلك إلى أن المصرح الذي تمارس فيه الجريمة الإلكترونية هونظام الحاسب الأولى، فالفاعل يستطيع أن يطبق جريمته على أنظمة مماثلة وذلك قبل تنفيذ الجريمة

ثالثا: الوسيلة

ويراد بها الإمكانيات التي يحتاجها المجرم الإلكتروني لإتمام جريمته، وهذه الوسائل قد تكون في غالب الأحيان، وسائل بسيطة وسهلة الحصول عليها خصوصا إذا كان النظام الذي يعمل بة الكمبيوتر من الأنظمة الشائعة أما إذا كان النظام من الأنظمة غير المألوفة، فتكون هذه الوسائل معقدة وعلى قدر من الصعوبة.

رابعا: السلطة

يقصد بالسلطة، الحقوق والمزايا التي يتمتع بها المجرم الإلكتروني والتي تمكنه من ارتكاب جريمته، فكثير من مجرمي المعلوماتية لديهم سلطة مباشرة أوغير مباشرة في مواجهة المعلومات محل الجريمة.

وقد تتمثل هذه السلطة في الشفرة الخاصة بالدخول إلى النظام الذي يحتوى على المعلومات وأيضا قد تكون السلطة عبارة عن حق الجاني في الدخول إلى الحاسب الالى وإجراء المعاملات، كما أن السلطة قد تكون شرعية من الممكن أن تكون غير شرعية كما في حالة سرقة شفرة الدخول الخاصة بشخص آخر.

خامسا: الباعث

وهوالرغبة في تحقيق الربح المادي بطريقة غير مشروعة ويضل هوالباعث الأول وراء ارتكاب الجريمة المعلوماتية ، . ويرى البعض أيضا ما يخالف ذلك في أن الربح المادي لا يعد هوالباعث في أغلب الأحيان على ارتكاب جرائم المعلوماتية وإنما هناك أمور عديدة أخرى في الغالب تكون هي الباعث مثل الانتقام من رب العمل، وأيضا مجرد الرغبة في قهر نظام الحاسب واختراق حاجزة الأمني. (**Francillon, 1990**).

المبحث الثاني :التحقيق الابتدائي في الجرائم الإلكترونية، ضبط الجريمة الإلكترونية والتحري، الادلة الرقمية تعريفها وجمعها وحجيتها وتوثيق وتوصيف الدليل الرقمي وتوصيات للحماية من الجرائم الإلكترونية

التحقيق في الجرائم الإلكترونية:

تستدعي خصوصية الجرائم الإلكترونية تطوير أساليب التحقيق الجنائي وإجراءاته وتمكن أجهزة القضاء والشرطة من كشف الجريمة وتعرف مرتكبيها بالسرعة والدقة اللازمتين ولابد لتحقيق ذلك من القيام بـ : تدريب الكوادر التي تباشر التحريات والتحقيقات، تطوير الإجراءات الجنائية، وتقتضي طبيعة الجرائم الإلكترونية معرفة متميزة بمكونات الحاسب الآلي ونظمه التعامل مع خدمة الإنترنت وأدوات وأساليب ارتكابها كما تقتضي معرفة أهم وكيفية تشغيلها كما تقتضي أيضا معرفة أساسيات عمل شبكات الحاسب الآلي وأهم مصطلحاتها وإجادة التعامل مع خدمة الانترنت وأدوات وأساليب ارتكابها كما تقتضي معرفة أهم تقنيات أمن الحاسوب والإنترنت وأدواتها وطريقة عملها، ومما لا شك فيه أن هذه المعرفة لن تتحقق إلا من خلال العمل على تدريب القائمين على أعمال التحرر والمباشرين للتحقيق في الجرائم الإلكترونية، الأمر الذي دفع ببعض الفقهاء إلى القول بضرورة وجود شرطة متخصصة ونيابة عامة متخصصة في هذا المجال .

وفي جميع الأحوال يمكن القول إن التدريب لا يمنع رجال الشرطة والقضاء من الاستعانة بأصحاب الخبرة الفنية المتميزة في مجال الحاسب الآلي وذلك بفرض كشف غموض الجرائم الإلكترونية وجمع أدلتها والحفاظ عليها، ذلك أن الإستعانة

بأصحاب الخبرة في المسائل الفنية البحتة ومنها الجرائم الإلكترونية هوأمر ملزم للقاضي الجزائي الذي لايملك القطع فيها دون استطلاع رأي أهل الخبرة والمعرفة، وإلا كان حكمه معيباً مستوجباً للنقض .

التحقيق الابتدائي في الجرائم الإلكترونية:

ثمة مجموعة من الاجراءات يجب إتباعها في هذا الإطار لاستحصال الدليل على الجريمة، وسنتناول في هذا الفرع التفتيش والخبرة فقط لكونهما أكثر الإجراءات تماساً وأهمية في نطاق الجريمة الإلكترونية:

أولاً: التفتيش: يُقصد بالتفتيش البحث عن جسم الجريمة والأداة التي استخدمت في إرتكابها وكل ماله علاقة بها أوبفاعلها

إن عالم تقنية المعلومات يتكون بطبيعة الحال من شقين هما الكيانات المادية والكيانات المعنوية، وتبعاً لذلك فإن التفتيش باعتباره اجراء من اجراءات التحقيق الابتدائي يختلف في كلا الشقين، وعلى ذلك لا بُد من التفريق بين تفتيش الكيانات المادية وتفتيش الكيانات المعنوية وذلك في النقطتين الآتيتين:

أ) تفتيش الكيانات المادية: إن التفتيش المتعلق بالكيانات المادية في نطاق الجرائم الإلكترونية يسهل إجراؤه وتنطبق عليه القواعد التقليدية للتفتيش، إذ لاخلاف على إن الولوج إلى المكونات المادية للكمبيوتر بحثاً عن شيء ما يتصل بجريمة معلوماتية وقعت يُفيد في كشف الحقيقة عنها وعن مرتكبها يخضع للاجراءات القانونية الخاصة بالتفتيش، بمعنى إن حكم تفتيش تلك المكونات المادية يتوقف على طبيعة المكان الموجودة فيه تلك المكونات وهل هومن الأماكن العامة أومن الأماكن الخاصة، حيث إن لصفة المكان وطبيعته أهمية قصوى خاصة في مجال

التفتيش، فإذا كانت موجودة في مكان خاص كمسكن المتهم أوأحد ملحقاته كان لها حرمة، فلا يجوز تفتيشها إلا في الحالات التي يجوز فيها التفتيش وبنفس الاجراءات المقررة قانوناً في التشريعات المختلفة، مع مراعاة التمييز بين ما إذا كانت مكونات الكمبيوتر المراد تفتيشها منعزلة عن غيرها من أجهزة الكمبيوتر الأخرى، أم إنها متصلة بكمبيوتر آخر أوبنهاية طرفية في مكان آخر كمسكن غير المتهم مثلاً، فإذا كانت كذلك وكانت هناك بيانات مخزنة في أوعية هذا النظام الأخير من شأنها كشف الحقيقة تعين مراعاة القيود التي يستلزمها المشرع لتفتيش هذه الأماكن، أما إذا وجد شخص يحمل مكونات الكمبيوتر المادية أوكان مسيطراً عليها أوحائزاً لها في مكان ما من الأماكن العامة سواء كانت عامة بطبيعتها كالطرق العامة والميادين والشوارع، أم كانت من الأماكن العامة بالتخصيص كالمقاهي والمطاعم والسيارات العامة، فإن تفتيشها لا يكون الا في الحالة التي يجوز فيها تفتيش الاشخاص وبنفس القيود المنصوص عليها في هذا المجال

ب) تفتيش الكيانات المعنوية: أثار تفتيش الكيانات المعنوية خلافاً كبيراً في الفقه، فذهب رأي في الفقه إلى جواز تفتيش وضبط البيانات الإلكترونية بمختلف أشكالها، ويستند هذا الرأي في ذلك إلى القوانين الإجرائية عندما تنص على إصدار الإذن بضبط (أي شيء)، فإن ذلك يجب تفسيره بحيث يشمل بيانات الكمبيوتر المحسوسة وغير المحسوسة، بينما ذهب رأي آخر إلى عدم انطباق المفهوم المادي على بيانات الحاسب غير المرئية أوغير الملموسة، ولذلك فإنه يقترح أصحاب هذا الرأي على مواجهة هذا القصور التشريعي بالنص صراحةً على جواز تفتيش المكونات المعنوية للكمبيوتر (إبراهيم، 2010)

وإذا ما تصفحنا المـواد الخاصـة بـالتفتيش في قـانون أصـول المحـاكمات الجزائيـة العراقي سنجد إن المشرع قد ذكر كلمة (أشياء)عـلى إطلاقهـا في أكـثر مـن موضـع في هذه المواد، وهذا يعني إن التفتيش في نطاق الجرائم الإلكترونية من الجـائز أن يمتـد للكيانات المادية والمعنوية على حد سواء ضـمن ضـوابط يجـب مراعاتهـا عنـد اجـراء التفتيش على هذه الكيانات

ثانياً: الخبرة: يقوم المحقق الجنـائي في مجـال الكشـف عـن غمـوض الجريمـة وفاعلهـا باتخـاذ الاجـراءات والوسـائل المتنوعـة اللازمـة لتحقيـق هدفـه، ومـن ضـمن هـذه الاجراءات هي الاستعانة بأهل الخبرة وذلك تحقيقـاً لمبـدأ هـام وهومبـدأ التخصـص نظراً لكون الخبرة هي تقدير مـادي أوذهنـي يُبديـه أصـحاب الفـن أوالإختصـاص في مسألة فنية لا يستطيع القائم بالتحقيق في الجريمة معرفتها وبمعلوماته الخاصة سواء أكانـت تلـك المسـألة الفنيـة متعلقـة بشـخص المـتهم أم بجسـم الجريمـة أم المـواد المستعملة في ارتكابها أم آثارها (العكيلي وحربة، 2009)

إن تشكيل فريق متخصص بالتحقيق في الجرائم بشكل عام قد يعد أمراً ضرورياً، ومرجع تقدير ذلك للجهة التحقيقية، أما عـلى مسـتوى الجـرائم الإلكترونيـة فـالأمر مختلف، إذ يُعد تشكيل مثل هكذا فريق مـن الاعتبـارات التـي لا منـاص منهـا ولـه أهمية خاصة نظراً للطبيعة الخاصة التي تتميز بها الجرائم الإلكترونية عن غيرها من الجرائم، وذلك لأن هذه الجرائم مرتبطة بمسائل فنية وعلمية بحتة، إذاً يصبح لزامـاً على القـائم بـالتحقيق الاسـتعانة بـالخبراء والمختصـين، لأن تصـدي المحقـق لفحـص شيء وإبداء الرأي فيه دون أن تتوافر لديه المعرفة اللازمـة يجعـل قـراره معيبـاً يضر بمصلحة التحقيق ويعوق الوصول إلى الحقيقة، وكل هـذا يصـب في أهميـة التقـارير

التي يُنجزها خبراء تقنية المعلومات في مجال الجرائم الإلكترونية ويُعطيها مكانة متميزة من حيث الإلزام.

إن إختيار الخبير في الجرائم الإلكترونية يتوقف على نوع الجريمة المرتكبة ومجال الخبرة المطلوبة وطبيعتها الفنية، فلا يكفي حصول الخبير على درجة علمية معينة، وإنما ينبغي أن تكون لديه خبرة علمية تخصصية وكفاءة فنية عالية في حقل أوأكثر من حقول تقنية المعلومات ونظمها ووسائلها، فقد تكون الجريمة المرتكبة تزوير مستندات أوتلاعباً في البيانات أوالغش أثناء نقل أوبث البيانات أوإطلاق الفيروسات أوقرصنة أوإعتداء على حرمة الحياة الخاصة أوالتجسس (إبراهيم، 2010)

تطوير الإجراءات الجنائية:

يستلزم التحقيق في الجرائم الإلكترونية العمل على تطوير إجراءات المعاينة والتفتيش والضبط والشهادة وذلك على النحوالتالي :

1- المعاينة: من الناحية القانونية هي مشاهدة وإثبات الحالة القائمة في مكان الجريمة والأشياء التي تتعلق بها .

2- التفتيش: هوالإجراء الذي يقوم به مأمور الضبط القضائي في الأحوال المعنية بالقانون بحثاً عن أدلة الجريمة .

3- الضبط: البيانات الإلكترونية ما هي إلا ذبذبات إلكترونية أوموجات كهرومغناطيسية تقبل الحفظ والتخزين على وسائط مادية وبالإمكان نقلها وبثها وإستقبالها وإعادة إنتاجها وبالتالي لا يمكن إنكار وجودها .

4- الشهادة: لا تختلف ما هي الشهادة في مجال الجريمة الإلكترونية عنها في الجريمة التقليدية فأمر سماع الشهود متروك.

إنَّ ظاهرة الجرائم الإلكترونية ظاهرة إجرامية مُستجدَّة نِسبيًّا تقرع في جنباتها أجراس الخطر لتنبِّه مجتمعات العصر الرّاهن لحجم المخاطر، وهول الخسائر الناجمة عنها، باعتبارها تستهدف الاعتداء على المعطيات بدلالتها التقنية الواسعة: بيانات، ومعلومات، وبرامج بكافّة أنواعها؛ فهي جريمة تقنية تنشأ في الخفاء، يقترفها مجرمون أذكياء، يمتلكون أدوات المعرفة التقنية، تُوَجَّه للنَّيْل مِنَ الحق في المعلومات، وتَطَال اعتداءاتها معطيات الكمبيوتر المخزَّنة، والمعلومات المنقولة، عبر نُظُم وشبكات المعلومات، وفي مقدمتها الإنترنت

مع تطور العالم حالياً في المجال التقني ظهرت جرائم المعلوماتية أوجرائم الكمبيوتر أوجرائم الحاسوب، وهي واحدة من الجرائم الخطيرة بما تسببه من خسائر جمة فضلاً عن صعوبة إثباتها والترف علي مرتكبيها، كما أنها لا تحتاج في إرتكابها لأكثر من البراعة في إستخدام أجهزة الحاسوب لذا فإن مرتكبيها تتفاوت أعمارهم ودوافعهم لإرتكاب هذه الجرائم (حجازي، 2005)

ضبط الجريمة المعلوماتية:

يعتمد ضبط الجريمة وإثباتها في المقام الأول على جمع ألادلة التي حدد المشرع وسائل إثباتها على سبيل الحصر، وذلك لما فيها من مساس بحرية الأفراد وحقوقهم الأساسية، فلا يجوز أن تخرج الأدلة التي يتم تجميعها عن تلك التي اعترف لها المشرع بالقيمة القانونية، وتتمثل في وسائل الإثبات الرئيسية وفي المعاينة والخبرة والتفتيش وضبط الأشياء المتعلقة بالجريمة، أما غيرها من وسائل الإثبات كالاستجواب والمواجهة وسماع الشهود فهي مرحلة تالية من إجراءات التحقيق وجمع الأدلة، ولما كنا بصدد تناول الجريمة المعلوماتية وما تثيره من مشكلات

إجرائية، فسنتعرض للمشكلات القانونية التي يثيرها إثبات هذه الجـرائم دون غيرهـا مـن الاجـراءات كالاسـتجواب والمواجهـة وسـماع الشـهود، لأن هـذه الأخـيرة تـتم في مواجهة البشر، أما المعاينة والخبرة والتفتيش ، فهي إجـراءات فنيـة محلهـا الأشـياء لا الافراد وهوما يهمنا في هذا الموضوع .

المخرجات الآليكترونية في الإثبات:

تخضع المحررات كغيرها مـن الأدلـة التـي تقـدم أثنـاء نظـر الـدعوى إلى تقـدير المحكمة حيث يسود مبـدأ حريـة القـاضي في تكـوين عقيدتـه، وهوما يختلـف فيـه القاضي المدني حيث يتقيد هذا الاخير بطرق معينـة في الإثبـات، فالقـاضي الجنـائي لـه مطلق الحرية في تقدير الدليل المطروح أمامه ، وله أن يأخذ بـه أويطرحـه ولا يجـوز تقييده بأي قرائن أوافتراضات.(سلامة، 2000)

ولما كانت المحررات أحد ألأدلة التي قد يلجأ اليها القاضي في الإثبات فهي تخضـع كغيرها من الادلة لتقدير المحكمة، الا إذا كان الإثبات متعلقاً بمواد غير جنائية، ففـي هذه الحالة يكون على القـاضي الجنـائي أن يتقيـد بطريـق الإثبـات المحـددة في ذلـك الفرع من القانون مثال ذلك حـق الملكيـة في جريمـة السرقـة ، والعقـود التـي تثبـت التصرف في الحق في جريمة خيانة الامانة أوصفة التاجر في جريمة التفـالس بالتـدليس (سلامة، 2000)

وهنا تثور مشكلة مدى حجية المخرجات الآليكترونية في الإثبات الجنائي في هـذه الحالات، فللمخرجات الآليكترونية انواع مختلفة، فهي تتنـوع بـين مخرجـات ورقيـة، ومخرجـات لاورقيـة وهـي المعلومـات المسـجلة عـلى الأوعيـة الممغنطـة كالاشرطـة والاقراص المرنة **Floppy Disk** القـرص الصـلب **Hard Disk** وغيرهـا مـن الاوعيـة

التي اصبحت في تطور مستمر حتى وصلت إلى اقراص ال**flash discs** التي اصبحت تتميز بسعات كبيرة للتخزين، خاصة أنه تواجهنا مشكلة اساسية تتعلق بصعوبة التمييز بين المحرر وصورته أوبين الاصل والصورة، ذلك لأننا نتعامل مع بيئة اليكترونية تعمل بالنبضات ووالذبذبات والرموز والأرقام وهوما يستحيل معه تطبيق القواعد الخاصة بالمحررات العرفية (شرف الدين، 2007)

الخبرة والمعاينة في الجرائم المعلوماتية:

تعتبر كل من الخبرة والمعاينة أكبر العقبات التي تواجه الإثبات في الجرائم المعلوماتية، فالمعاينة اجراء بمقتضاه ينتقل المحقق إلى مكان وقوع الجريمة ليشاهد اثارها بنفسه، فيقوم بجمعها وجمع أي شيء يفيد في كشف الحقيقة، وتقتضي المعاينة إثبات حالة الأشخاص والأشياء الموجودة بمكان الجريمة ورفع الآثار المتعلقة بها كالبصمات والدماء وغيرها مما يفيد التحقيق، والمعاينة تكون شخصية إذا تعلقت بشخص المجني عليه، أومكانية اذا تعلقت بالمكان الذي تمت فيه الجريمة، ووضع الشهود والمتهم والمجني عليه، أما المعاينة العينية فهي التي تتعلق بالأشياء أو الأدوات المستخدمة في ارتكاب الجريمة وقد يقتضي الأمر الاستعانة بخبير للتعرف على طبيعة المادة اونوعها إذا كان ذلك يحتاج لرأي المتخصص، وفي هذه الحالة يتم ارسال هذه الاشياء إلى الخبير لنكون امام بصدد اجراء آخر من اجراءات التحقيق وهوالخبرة، فالخبرة هي أحد أهم وسائل جمع الأدلة، يلجأ اليها المحقق عند وجود واقعة مادية أوشيء مادي يحتاج االتعرف عليه إلى حكم الخبير المتخصص، فهويأخذ حكم الشاهد من حيث الحجية أوالقوة في الإثبات.

أما السلوك الإجرامي في في الجريمة المعلوماتية فهوعبارة عن بيانات مخزنة في نظام معلوماتي يتطلب إثباته انتقال محقق متخصص حيث يتم التفتيش عن البيانات

عن طريق نقل محتويات الاسطوانة الصلبة الخاصة بالجهاز، ويجب على المحقق أوضباط الشرطة المتخصصين استخراج المعلومات التي من شأنها أن تساعد التحقيق وأن يطلعوا زملائهم عليها، مثل القيام بالبحث في بنوك المعلومات وفحص كل الوثائق المحفوظة ومراسلات مرتكب الجريمة مثل الرسائل الإلكترونية وفك شفرات الرسائل المشفرة. وهوما يحدث عندما ترتكب الجريمة عبر شبكة الانترنت، ولكي ينجح المحققون في عملهم يجب أن يقتفوا أثر الاتصالات منذ الحاسب المصدر إلى الحاسب أوالمعدات الأخرى التي تملكها الضحية، مروراً بمؤدي الخدمة والوساطة في كل ودولة. كما يقتضي ذلك أيضا ان يعمل المحقق على الوصول إلى الملفات التاريخية التي تبين لحظات مختلف الاتصالات. من أين صدرت؟ ومن الذي يحتمل إجراؤها، بالإضافة إلى ضرورة المام المحقق بالحالات التي يكون عليه فيها التحفظ على الجهاز أوالاكتفاء بأخذ نسخة من الاسطوانة الصلبة للحاسب، والاوقات التي يستخدم فيها برامج استعادة المعلومات التي تم الغاؤها (البربري، 2001)

فالمحقق الذي يقوم بمعاينة الجريمة المعلوماتية يجب أن يكون ملماً بمهرات هذه التقنية، مثل القدرة على استخدام برامج **Time stamp** وهي البرامج التي يمكن عن طريقها تحديد الزمن الذي تم فيه السلوك الإجرامي، لأن ذلك لا يكون متاحاً في جميع الأنظمة المعلوماتية ، أما الخبير ففي هذه الحالة يجب ان يكون ملماً بمهارات تحليل البيانات ومهارات التشفير **cryptanalysis skills** التي تتيح له فك الرموز استعادة البيانات الملغية .

إجراءات الإثبات:

إن المحققين يُواجهون العديد من الصعوبات عند ممارسة وظائفهم في إثبات الجرائم الإلكترونية وهوما يتطلب مجهوداً إضافياً وتدريباً وتعاوناً من الجهات ذات العلاقة لإثبات هذا النوع من الجرائم.

التحري وجمع الأدلة في الجرائم الإلكترونية:

عادةً ما تبقى الجريمة مستترة حتى يصل خبرها إلى السلطات المختصة، هذا الوضع ينطبق على الجرائم كافة دون استثناء، لكنه يتجلى وضوحاً بالنسبة لجرائم تقنية المعلومات نظراً لطبيعتها، حيث يصعب على الأشخاص العاديين الإبلاغ عنها لما تتطلبه من مهارات فنية غير متوافرة سوى لفئات مهنية أوتخصصية في مجال الحاسب الآلي ونظم تقنية المعلومات، وفي الأحوال جميعها فإن أي إخبار عن جريمة سواء كان فاعلها مجهولاً أم معلوماً ينبغي أن يتضمن على الأقل معلومات أولية عن الجريمة مثل تحديد محل الجريمة ومكان وقوعها ونوعها، إذ تُعد هذه العناصر مهمة وضرورية لمساعدة رجال الضبط القضائي في أي إخبار متعلق بجرائم تقنية المعلومات، بحيث تُمكنهم من تحديد معالم الجريمة ووضع خطة للتعامل معها من الناحيتين الفنية والقانونية.

هذا ويتم الكشف عن الجرائم الإلكترونية بوضع برمجيات حاسوبية معينة خصوصاً فيما يخص جرائم القرصنة أونشر المواد الإباحية.

إن استحداث الأدوات البرمجية الحاسوبية التي من خلالها يُمكن التعرف على الأنماط الإجرامية تعد مسألة لا غنى عنها في كشف الجريمة بالنظر لضخامة حجم المعلومات المتوافرة في شبكة الانترنت، وهناك وسيلتان لأعضاء الضبط القضائي

لغرض الحصول على البيانات المتعلقة بارتكاب الجريمة من نظام حاسوب، وهما تستندان إلى معايير تقنية وقانونية، وتتمثل بما يأتي:

1. يتم الحصول على المعلومات من الموقع نفسه الذي تم من خلاله ارتكاب الجريمة بعد أن يتم اكتشافه باستخدام البرمجيات الحديثة.
2. يتم الحصول على المعلومات عن طريق إعتراض أورصد البيانات المنقولة من الموقع أوإليه أوفي إطاره (الحيدري ، 2012)

أما إذا كانت الجريمة مشهودة كما لوتم ضبط الفاعل وهويستخدم موقع الانترنت لارتكاب إحدى الجرائم، فعلى عضوالضبط القضائي إخبار قاضي التحقيق والادعاء العام بوقوع الجريمة وينتقل فوراً إلى محل الحادثة ويسأل المتهم عن التهمة المُسندة إليه ويضبط كل ما يظهر إنه استعمل في إرتكاب الجريمة من مخرجات ورقية وشرائط وأقراص ممغنطة وغيرها من الأشياء التي يُعتقد إن لها صلة بالجريمة ويسمع أقوال من يُمكن الحصول منه على معلومات وأيضاحات في شأن الحادثة ومرتكبها ويُنظم محضراً بذلك، وبشكل عام على المكلفين بمعاينة مسرح الجريمة اتباع جملة من الارشادات التي قد تسهم بإزالة الغموض المحيط بملابسات ارتكاب الجريمة (إبراهيم، 2010):

1. التحفظ على الأجهزة وملحقاتها والمستندات الموجودة من مخرجات ورقية وشرائط وأقراص ممغنطة وغيرها من الاشياء التي يعتقد ان لها صلة بالجريمة.
2. إثبات الطريقة التي تم بواسطتها اعداد النظام والعمليات الإلكترونية، وخاصة ما تحتويه السجلات الإلكترونية التي تزود بها شبكات المعلومات لمعرفة موقع الاتصال ونوع الجهاز الذي تم عن طريقه الدخول إلى النظام.

3. عدم نقل أي مادة متحفظ عليها من مسرح الجريمة قبل التأكد من خلوالمحيط الخارجي بموقع الحاسب الآلي من أي مجالات لقوة مغناطيسية يُمكن أن تسبب في محوالبيانات المسجلة عليها.
4. إثبات حالة التوصيلات والكابلات المتصلة بمكونات النظام كله، وذلك لا جراء مقارنة لدى عرض الأمر على القضاء.

مفهوم الدليل الجنائي الرقمي وحجيته في الإثبات:

- **أدلة الجريمة الإلكترونية :**

يمكن القول إن الدليل الجنائي هوكل ما يمكن الحصول عليه بواسطة إجراءات قانونية أووسائل فنية أومادية أوقولية، بهدف استخدامه في أي مرحلة من مراحل التحقيق في حل لغز الجريمة الواقعة ومن ثم نسبتها أوعدم نسبتها إلى المشتبه به وبما أن الحديث يدور في فلك الجرائم الإلكترونية فإن عملية الإثبات الجنائي لهذا النوع من الجرائم الإلكترونية، يرى بعض الفقهاء أن الأدلة الجنائية الرقمية ما هي إلا مرحلة متقدمة من الأدلة المادية الملموسة، التي يمكن إدراكها بإحدى حواس الإنسان الطبيعية من خلال الاستعانة بما ابتكره العلم الحديث من وسائل التقانة العالية والتي من ضمنها الحاسب الآلي، الذي هومحور الأدلة الرقمية وجوهرها في حين يرى بعضهم الآخر أن الأدلة الرقمية هي نوع متميز من وسائل الإثبات، له من الخصائص العلمية والمواصفات القانونية ما يؤهله ليكون نوعاً جديداً من الأدلة.

- **مفهوم الدليل الجنائي الرقمي:**

يلعب الدليل الجنائي بشكل عام دورًا هامًا، في ظهور الحقيقة المُتعلقة بالوقائع محل التحقيق أوالمُحاكمة، وهوحجر الأساس الذي تقوم عليه الدعوى في كثير من الأحيان، كما يلعب الدليل الجنائي دورًا محوريًا في تكوين عقيدة القاضي.

- **تعريف مفهوم الدليل الرقمي بأنه**

أي معلومات الكترونية لها قوة، اوقيمة ثبوتية مخزنة اومنقولة، اومستخرجة اومأخوذة من اجهزة الحاسب اوالشبكات المعلوماتية وما في حكمها ويمكن تجميعها وتحليلها باستخدام اجهزة اوبرامج اوتطبيقات تكنولوجية خاصة(قانون مكافحة جرائم تقنية المعلومات المصري مادة رقم 1 قانون رقم 175 صادر عام 2018.

ويُلاحظ بداية، أن السياق الذي أتى خلاله هذا التعريف يُفهم منه أن مفهوم الدليل الجنائي الرقمي وما يجب أن يتوفر فيه من ضوابط وشروط تحقُق، تقتصر فقط على ما يتعلق بنطاق تطبيق قانون مكافحة جرائم تقنية المعلومات، فالتعريفات التي وردت بالمادة الأولى من قانون الجريمة الإلكترونية ترتبط بتطبيق أحكام قانون الجريمة الإلكترونية فقط، حسب ظاهر النص، لكن من الوارد أن نجد في التطبيقات العملية، أن المحاكم المصرية قد تتوسع في استخدام تعريف الدليل الرقمي الوارد بقانون مكافحة جرائم تقنية المعلومات، نظرًا لأن القوانين الإجرائية، مثل قانون الإجراءات الجنائية، لم تتضمن حتى الآن تعريفًا لمفهوم الدليل الجنائي الرقمي.

وبشكل عام جاء تعريف الدليل الرقمي في صياغة شديدة العمومية، بما يسمح إجرائيًا بالتوسع فيما يُمكن اعتباره دليًلا رقميًا، ولم يضع التعريف الوارد بقانون مُكافحة جرائم تقنية معلومات سوى ضابطين يتعلقان بالمعلومات التي يتم جمعها أواستخراجها من الأجهزة والشبكات، ونرى أن العنصرين اللذان تم ذكرهما أساسين يُكمل كل منهما الآخر، لذا يجب توفرهما معًا، ويجب أن أيضا أن يستمر توفرهما في الدليل على الأقل في المرحلة الخاصة بجمع واستخراج الدليل ومرحلة توثيق وتوصيف الدليل.

القوة الثبوتية للمعلومات المُستخرجة: يرتبط العنصر الأول الذي تضمنه تعريف الدليل الجنائي الرقمي بثبوتية المعلومات المخزنة أوالمنقولة أوالمستخرجة أوالمأخوذة من أجهزة الحاسب أوالشبكات المعلوماتية، ويفهم ضمنيًا من القوة الثبوتية، أن المقصود هوقدرة المعلومات التي تم الحصول عليها في إثبات ارتكاب الجريمة أمام الجهات القضائية، كما يُفهم من التعريف أن استخراج الدليل وجمعه لا يقتصر على أجهزة الحاسب فقط، حيث أستخدم التعريف عبارة " وما في حكمها" وهوما يعني أن التعريف يعتبر أن أي أجهزة اوشبكات، يمكن الاعتداد بها كدليل جنائي رقمي، مدام لدى هذه الاجهزة والشبكات القدرة على تخزين البيانات والمعلومات.

إمكانية جمع وتحليل المعلومات المُستخرجة: أما عن العنصر الثاني الذي يجب توافره بجانب قوة ثبوتية المعلومات المستخرجة فهوإمكانية تجميع وتحليل هذه المعلومات باستخدام أجهزة أوبرامج أوتطبيقات تكنولوجية خاصة، وقد حددت اللائحة التنفيذية لقانون مُكافحة جرائم تقنية المعلومات الخواص التي يجب أن تتمتع بها البرامج التي يُمكن استخدامها في عملية جمع أوالحصول أواستخراج المعلومات، ومن أهمها الخواص أوالإمكانيات التي تضمن عدم تغيير أوتحديث أومحوأوتحريف للكتابة أوالبيانات والمعلومات، وقد حددت اللائحة نوعين من البرامج تم ذكرهم على سبيل المثال **Digital Images HashK, Write Blocker**.

الجهة المسئولة عن جمع الدليل الرقمي:

يمر الحصول عل الدليل الجنائي الرقمي بمراحل مُتعددة، من بينها (جمع الدليل الرقمي - استخراجه- حفظه- تحريزه - توثيقه وتوصيفه) لذلك حددت اللائحة

التنفيذية لقانون مُكافحة جرائم تقنية المعلومات، الجهات المسؤولة عن القيام بهـذه الاجراءات، حيث قُصرت هذه الاجراءات على فئتين.

- الفئة الأولى وهم مأموري الضبط القضائي، وقـد أشـارت اللائحـة بشـكل عـام إلى ضرورة أن يكـون مـأموري الضـبط القضـائي الـذين يقومـوا بـأي مـن الإجـراءات المُتعلقة بالدليل الرقمي من المخـول لهـم التعامـل في هـذه النوعيـة مـن الأدلـة، ويفهم من ذلك أنـه فـيما عـدا مـأموري الضـبط المُختصـين أوالصـادر لهـم قـرار بالضبطية القضائية في الجرائم المُنصوص عليها بقانون جرائم تقنية المعلومـات لا يحق لأي مأمور قضائي جمع الدليل الرقمي أواستخراجه أوحفظه أوتحريزه ومـن ثم تحرير محاضر الضبط المتعلقة بالأدلة.
- أما الفئة الثانية وهم الخبراء المُتخصصين، فقد أعطت اللائحة للخبراء المتخصصـين الحق في جمع الدليل الرقمـي واسـتخراجه وحفظـه وتحريـزه، وتحريـر التقـارير الفنية المُرتبطـة بهـذه الإجـراءات، وتجـدر المُلاحظـة أن الأصـل في عمـل الخـبراء المُتخصصين في عملية جمع الدليل الرقمي واستخراجه وحفظه وتحريزه، يتم بُناء على انتداب هؤلاء الخبراء للقيام بهـذه المهـام مـن جهـات التحقيـق أوالمحاكمـة فقط(قانون مكافحة جرائم تقنية المعلومات المصري ماده رقـم 10 قـانون رقـم 175 صادر عام 2018

بينما تعطى اللائحة التنفيذية للخبراء المُتخصصـين بعـض المهـام الفنيـة والتقنيـة الأخرى مثل أعمال التوصيف والتوثيق للأدلة الرقمية، وفي هذه الحالـة يقـوم الخـبراء بأداء مهام التوثيق والتوصيف وفقًا للتكليفات التي قد تصـدر مـن جهـات التحقيـق أوالجهات القضائية المُختصة أوالجهات المعنية بمكافحة جرائم تقنيـة المعلومـات، وفي هـذه الحالـة قـد يقـوم أحـد مـأموري الضـبط القضـائي بعمليـة جمـع اواسـتخراج

الدليل أوتحريزها بينما يترك للخبراء مهام توثيق وتوصيف الدليل الرقمي، إذا رأت الجهات المعنية بمكافحة جرائم تقنية المعلومات أن هناك حاجة لذلك.

حجية الدليل الرقمي في الإثبات الجنائي في الجرائم الرقمية:

تُثير حجية الدليل الرقمي، أهمية كبيرة فيما يتعلق بالدور الذي يلعبه الدليل الرقمي في إثبات الجريمة، لذلك يجب أن يتوافر في الدليل عناصر هامة، لكي يُمكن الاستناد إليه في عملية إثبات الجريمة.

وقد تناول قانون مكافحة جرائم تقنية المعلومات، المُحددات المتعلقة بحجية الدليل الجنائي المُرتبط بالجرائم المنصوص عليها بالقانون، حيث يُشير القانون إلى أن الأدلة المستمدة أوالمستخرجة من الأجهزة، أوالمعدات، أوالوسائط أوالدعامات الإلكترونية أومن النظام المعلوماتي أومن برامج الحاسب، أومن أي وسيلة لتقنية المعلومات، ذات قيمة وحجية الأدلة الجنائية المادية في الإثبات الجنائي.

ويشترط قانون مكافحة جرائم تنقية المعلومات، للأخذ بالدليل الرقمي واعتباره ذوحُجية في عملية الإثبات، توافر بعض الشروط الفنية في هذا الدليل، وقد أحال قانون مكافحة جرائم تقنية المعلومات توضيح هذه الضوابط والشروط إلى اللائحة التنفيذية للقانون(اللائحة التنفيذية لقانون مكافحة جرائم تقنية المعلومات المصري لعام 2020) ، والتي فسرت بدورها الضوابط والشروط الفنية التي يجب توافرها للاعتداد بالدليل الرقمي، ومن هذه الضوابط:

1- أن تتم عملية جمع أوالحصول على أواستخراج أواستنباط الادلة الرقمية محل الواقعة باستخدام التقنيات التي تضمن عدم تغيير أوتحديث أومحوأوتحريف للكتابة اوالبيانات والمعلومات، أوأنظمة المعلومات والبرامج، أوالدعامات

الإلكترونيـة وغيرهـا. ومنهـا عـلى الأخـص تقنيـة **Digital Images HashK,** **Write Blocker** ، وغيرها من التقنيات المماثلة.

2- أن تكون الأدلة الرقمية ذات صـلة بالواقعـة وفي إطـار الموضـوع المطلـوب إثباتـه أونفيه، وفقًا لنطاق قرار جهة التحقيق أوالمحكمة المختصة.

3- أن يتم جمع الدليل الرقمي واستخراجه وحفظه وتحريزه بمعرفة مأموري الضـبط القضائي المخول لهم التعامل في هـذه النوعيـة مـن الأدلـة، أوالخـبراء المُتخصصـين المنتـدبين مـن جهـات التحقيـق أوالمحاكمـة، عـلى أن يُبـين في محـاضر الضـبط، أوالتقارير الفنية على نوع ومواصفات البرامج والأدوات والأجهزة والمعـدات التـي تم استخدامها، مع توثيق كود وخوارزم **Hash** الناتج عن استخراج نسخة مُماثلة ومطابقة للأصل من الدليل الرقمي بمحضر الضبط أوتقريـر الفحـص الفنـي ومـع ضمان استمرار الأصل دون عبث به.

في حالة تعذر فحص نسخة الدليل الرقمي وعدم إمكانية الـتحفظ عـلى الاجهـزة محل الفحص لأي سبب يتم فحص الأصل ويثب ذلك كله في محضر الضبط أوتقريـر الفحص والتحليل.

4- أن يتم توثيق الأدلة الرقميـة بمـحضر إجـراءات مـن قبـل المخـتص قبـل عمليـات الفحص والتحليل له وكذا توثيق مكان ضبطه ومكان حفظه ومكان التعامل معه ومواصفاته.

ويجب الإشارة إلى أن الشروط والضوابط التي حددتها اللائحة التنفيذيـة لقـانون مُكافحة جرائم تقنية المعلومات، يجـب أن تتـوافر جميعهـا في الـدليل الرقمـي حتـى يكتسب حجية في عملية الإثبات الجنائي، وأن تخلف أحد هذه العناصر، يُفقد الدليل قوته اللازمـة للاحتجـاج بـه واسـتخدامه في عمليـة الإثبـات، ويجـب هنـا الإشـارة أن

فقدان هذه الشروط، تُفقد الدليل قدرته الكاملـة في عمليـة الإثبـات، إلا أن ذلـك لا يعني استبعاد ما أفضت إليه هذه العملية بالكامل، حيث يُمكن الأخذ بمـا أفضى إليـه الدليل، تحت توصيفات قانونية أخرى، ولكنها ليست بقوة الدليل الـذي ألـزم قـانون مكافحة جرائم تقنية المعلومات توفره.

طرق توصيف وتوثيق الدليل الرقمي:

(اللائحة التنفيذية لقانون مكافحة جرائم تقنية المعلومات المصري لعام 2020)

حسب ما جاء باللائحة التنفيذية لقانون مكافحة جـرائم تقنيـة المعلومـات فـإن مرحلة توثيق وتوصيف الدليل الجنـائي الرقمـي، تـأتي في مرحلـة لاحقـة عـلى عمليـة الجمع واستخراج الدليل، وهي مرحلة يتم فيها إنتـاج المعلومـات المُخزنـة عـلى أحـد الأجهزة أوالشبكات إلى معلومات في صورة نسخ مطبوعـة، وذلـك مـن خـلال طباعـة نسخ من الملفات المخزن عليها أوتصويرها بأي وسيلة مرئية أورقمية، وتشترط اللائحة في هذه المرحلة أن تكون النسخ المطبوعة من الدليل مدوّن عليها البيانات التالي:

- تاريخ وقت الطباعة والتصوير.
- اسم أونوع نظام التشغيل ورقم الإصدار الخاص به.
- اسم البرنامج ونوع الإصدار أوالاوامر المستعملة لعدد النسخ.
- البيانات والمعلومات الخاصة بمحتوى الدليل المضبوط.
- بيانات الاجهزة والمعدات والبرامج والأدوات المستخدمة.
- اعتماد (توقيع) الأشخاص القائمين عـلى جمـع أواسـتخراج أوالحصـول أوالتحليـل للأدلة الرقمية.

توصيات مهمه في الوقاية والحماية من الجرائم الرقمية:

الجرائم الرقمية هي جرائم ذات حداثة ومتطورة باستمرار وتتعدد اشكالها وصورها وتتطور بشكل سريع وقوي، ومن اجل المكافحة والوقاية من هذه الجرائم المستحدثة اوجز هما بعض التوصيات التي من شانها انها قد تساهم في الوقاية والحماية:

* إضافة منهاج إلى المناهج في المدارس والجامعات يعالج ويقوم الاستخدام الامثل للأنترنت (التربية الإلكترونية).)
* باستمرار يجب تطوير القوانين واللوائح والتنفيذية ونصوص التجريم المتعلقة باستعمال الشبكات العنكبوتية والانترنت، لبناء منظومة قانونيّة الأنظمة المعلوماتيّة المشروعة.
* إبتكار رخص حاسوبية تسمح للقائمين على مكافحة الجرائم الرقمية إجراء المعالجة فورا لإيقاف اوحذف حسابات تخريبية أو مواقع إباحية.
* زيادة وتطوير المعرفة الحاسوبية وتطبيقاته للقائمين في مجال الأمن والتعليم وتنمية مهاراتهم الحاسوبية.
* نشر الوعي بين المواطنين حول أخطار التعامل الخاطئ مع بعض الحسابات المزيفة ووبعض المواقع علي شبكة الإنترنت.
* نشر الوعي حول الآثار الناجمة الوقوع في الابتزاز الرقمي الإلكتروني والانجراف غير الاخلاقي.
* نشر الوعي بين فئة الآباء من أخطار الإنترنت على أطفالهم لحمايتهم من الوقع في أفخاخ الصيادين الرقميين.

* الفلترة الإلكترونية من قبل المكافحين للجرائم الرقمية حيث يتم فلترة البرامج والتطبيقات للتأكد من خلوها من أي محتوي غير شرعي.

* الحذر والحرص من تبادل الصور والخصوصيات والاحاديث الحميمة مع الاشخاص الاخرين.

* زيادة مساهمة وتشاركية الشباب والمواطنين ومؤسسات المجتمع المحلي والقطاع التعليمي في الواقعية من الجرائم الرقمية.

* تقديم العلاج والدعم والمساندة لمن يقع فريسة الجرائم الرقمية من قبل مؤسسات الدولة المعنية في المكافحة والوقاية من الجرائم الرقمية وبطريقة تحفظية سرية.

* زيادة التعاون الدولي وتوقيع البروتوكولات القانونية بين الدول للحماية والوقاية والمكافحة الدولية المشتركة من جرائم الحاسوب والقرصنة والاستغلال والابتزاز.

مراجع الفصل الثاني

1- المراجع العربية

1. د.هشام فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، أسيوط، 1992، ص5.
2. د. عمر عبدالعزيز موسى الدبور، آليات تفعيل الحماية والوقاية من الجرائم الإلكترونية: جامعة المنوفية مصر. كتاب أعمال مؤتمر الجرائم الإلكترونية المنعقد في طرابلس/ لبنان، يومي 24-25|03|2017، ص 215.
3. هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، مكتبة الآلات الحديثة، مصر، 2000، ص45.
4. د. هشام رستم – المرجع السابقٍ – ص29.
5. أ.د. صالح أحمد البربري - دور الشرطة في مكافحة جرائم الإنترنت في إطار الاتفاقية الأوروبية - الموقعة في بودابست في 2001/11/23 –www **.arablawinfo.com** - ص2
6. ممدوح خليل عمر – حماية الحياة الخاصة والقانون الجنائي – دار النهضة العربية القاهرة 1983 ص 207
7. أسامة عبد الله قايد – الحماية الجنائية للحياة الخاصة وبنوك المعلومات – دار النهضة العربية القاهرة 1994 ص 48
8. عبد الفتاح بيومي حجازي – صراع الكمبيوتر والانترنت – في القانون العربي النموذجي دار الكتب القانونية – القاهرة 2007 ص 609

9. بدر سليمان لويس – أثر التطور التكنولوجي مع الحريات الشخصية في النظم السياسية رسالة الدكتوراة – حقوق القاهرة 1982
10. عبد الفتاح بيومي حجازي - المرجع السابق ص 620
11. هشام فريد رستم – قانون العقوبات مخاطر المعلومات مكنة الآلات الحديثة أسيوط 1992ص 81
12. محمد سامي الشوا ثورة المعلومات وبعكسها على قانون العقوبات دار النهضة العربية القاهرة 1994ص 70-72 وما بعدها
13. محمد إبراهيم محمد الشافعي، النقود الإلكترونية، مجلة الأمن والحياة، أكاديمية الشرطة، دبي، س 12، ع1، يناير، 2004، ص142–148.
14. منير الجنبيهي – ممدوح الجنبيهي – البنوك الإلكترونية ط 2 – 2006 دار الفكر الجامعي – الإسكندرية ص47
15. عبد الفتاح بيومي حجازي – صراع الكمبيوتر والانترنت – في القانون العربي النموذجي دار الكتب القانونية – دار للنشر والبرمجيات – القاهرة 2007 ص 609
16. عبد الفتاح بيومي حجازي – جرائم الكمبيوتر والانترنت – دار الكتب القانونية – القاهرة 2005 ص 42
17. محمود نجيب حسني – شرح قانون العقوبات – القسم الخاص – الجرائم المضرة بالمصلحة العامة – دار النهضة العربية - القاهرة 1972 ص 322
18. محمد سامي الشوا – ثورة المعلومات وانعكاساتها على قانون العقوبات – دار النهضة العربية – القاهرة 1994 ص 155
19. حسن صادق المرصفاوي – قانون العقوبات الخاص – منشأة المعارف – الاسكندرية مصر 1991 ص 116

20. محمد سامي الشوا – المرجع السابق ص 155

21. ناصر بن محمد البقمي/مكافحة الجرائم المعلوماتية وتطبيقاتها في دول مجلس التعاون لدول الخليج العربية/سلسلة محاضرات الامارات تصدر عن مركز الامارات للدراسات والبحوث الاستراتيجية /العدد 2008/116 /ص10.

22. أحمد خليفة الملط/الجرائم المعلوماتية/دار الفكر الجامعي/ الإسكندرية /2005/ص 102.

23. ناصر بن محمد البقمي/مصدر سابق/ص11.

24. راشد بشير إبراهيم/التحقيق الجنائي في جرائم تقنية المعلومات (دراسة تطبيقية على امارة ابوظبي)/بحث منشور في مجلة دراسات استراتيجية/مركز الامارات للدراسات والبحوث الاستراتيجية/العدد 2008/131/ص23.

25. عبد الفتاح بيومي حجازي/مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي/ط1/دار الفكر الجامعي/الاسكندرية/2006/ص21.

26. جمال إبراهيم الحيدري/الجرائم الإلكترونية وسبل معالجتها/ط1/مكتبة السنهوري/بغداد/2012/ص30.

27. جمال إبراهيم الحيدري/الجرائم الإلكترونية وسبل معالجتها/ط1/مكتبة السنهوري/بغداد/2012/ص30.

28. خالد عياد الحلبي/مصدر سابق/ص223.

29. راشد بشير إبراهيم/مصدر سابق/ص90.

30. خالد عياد الحلبي/مصدر سابق/ص223.

31. خالد ممدوح إبراهيم/فن التحقيق الجنائي في الجرائم الإلكترونية/دار الفكر الجامعي/الاسكندرية/2010/ص67-68.

32. دراسة بعنوان (المعاهدات الدولية للانترنت:حقائق وتحديات)للدكتور(جورج لبكي) منشورة على الموقع الإلكتروني (**www.groups.google.com**).
33. يونس خالد عرب مصطفي، جرائم الحاسوب، دراسة مقارنة، رسالة ماجستير مقدمة إلى الجامعة الأردنية 1994، ص 72.
34. عبد الفتاح بيومي حجازي – جرائم الكمبيوتر والانترنت – دار الكتب القانونية – القاهرة 2005.
35. مأمون سلامة - الاجراءات الجنائية في التشريع الليبي – ج 2ط2000- منشورات المكتبة الجامعة – ص151
36. مأمون سلامة – المرجع السابق – ص160
37. احمد شرف الدين- حجية الرسائل الآليكترونية في الإثبات – شبكة المعلومات القانونية العربية – **East Law .com – 2007**
38. **Recommandations sur le dépistage des communications électroniques transfrontalière dans le cadre des enquêtes sur les activités criminelles www G8 Mont tremblant Canada 21 mai 2002**

أشار إليه أ.د. صالح أحمد البربري دور الشرطة في مكافحة جرائم الإنترنت في إطار الاتفاقية الأوروبية -الموقعة في بودابست في 2001/11/3- **www.@arablawinfo.com**

39. جمال إبراهيم الحيدري/مصدر سابق/ص76.
40. راشد بشير إبراهيم /مصدر سابق/ص52
41. عبد الأمير العكيلي، د.سليم حربة/ شرح قانون أصول المحاكمات الجزائية/ ج1/د.ن/بيروت/2009/ص126.
42. خالد ممدوح إبراهيم/مصدر سابق/ص197.

43. راشد بشير إبراهيم /مصدر سابق/ ص69.

44. قانون مكافحة جرائم تقنية المعلومات المصري رقم 175 الصادر عام 2018.

45. اللائحة التنفيذية لقانون مكافحة جرائم تقنية المعلومات المصري الصادرة عام 2020.

2- المراجع الأجنبية

1. **David Bainbridge- Introduction to computer law-third edition-Pit Man publishing1996 p237**
2. **Francillon ،Les crimes inormatiques et d'autres crimes dans le domaine de la technologie informatique en france Rev. int. pén ، ،1990vol 64 ،p. 293.**

الفصل الثالث

الجريمة السيبرانية

الفصل الثالث

الجريمة السيبرانية

المبحث الأول: ماهيــة الجريمــة الســيبرانية وانواعهــا وصــورها وتطورهــا وخصائصــها واسبابها وتكلفتها

مفهوم الجريمة السيبرانية:

الثورة المعلوماتية وصناعة المعلومات والتقدم التكنولوجي والانترنـت ساهـم في تطور متسارع في التواصل والاتصال ووسائل إبراز في جميع انحاء العالم وعـلى جميـع الصعد، الأمر الذي أدى إلى إفراز نوع جديد من الجرائم المعلوماتية والتـي كـان لهـا عدة مسميات منها جرائم الإنترنـت (**Computer crime**)، جـرائم التقنيـة العاليـة (**Hi-tech crime**)، الجريمـة السـيبرانية (**Cyber crime**) ، وثمـة تبـاين كبـير بشـأن المُصـطلحات المُسـتخدمة للدلالـة عـلى هـذه الظـاهرة الإجراميـة الناشـئة في العـالم الافتراضي.

تعتبر الجريمة السـيبرانية أي نـوع مـن الأنشـطة الإجراميـة التـي تـتم باسـتخدام التقنيات الحاسوبية والإلكترونية، كما أنهـا تسـتهدف الأنظمـة السـيبرانية والشـبكات والبيانات الإلكترونية،

ويمكن تعريف الجريمة السيبرانية على أنها أي نشاط إجرامي يتم باستخدام التقنيات الحاسوبية والإلكترونية، ويستهدف الأنظمة السيبرانية والشبكات والبيانات الإلكترونية.

كما يتمثل في اختراق الأنظمة وسرقة المعلومات وتدميرها وتعطيلها والاحتيال والتجسس والإساءة والابتزاز وغيرها من الأنشطة الإجرامية التي تتم باستخدام التقنيات الحاسوبية والإلكترونية.

وكما أنه هذه الجرائم تتسم بأنها تتم بشكل سريع ومن دون وجود أدلة مادية، مما يجعل من الصعب التحقيق فيها ومحاسبة المتسببين فيها.

كما تشكل الجرائم السيبرانية تهديدًا خطيرًا للأمن السيبراني والاقتصاد الرقمي في جميع أنحاء العالم، وتتطلب جهودًا كبيرة للحد منها والحفاظ على الأمان والسلامة في الفضاء السيبراني.

لذلك يمكننا الرجوع إلى تعريف محمد الرشيد، في كتابه أمن المعلومات والذي يعد من أهم الكتب العربية في مجال أمن المعلومات.

حيث قام بتعريف الجريمة السيبرانية على النحوالتالي:

"هي أي نشاط إجرامي يتم باستخدام التقنيات الحاسوبية والشبكات الإلكترونية والأنظمة السيبرانية، يهدف إلى الحصول على المعلومات أوالتلاعب بها أوتدميرها أوإيذاء الأفراد أوالمؤسسات، أوالإضرار بالأنظمة السيبرانية، ويتميز بأنه يتم بشكل سريع ومن دون وجود أدلة مادية، مما يجعل من الصعب التحقيق فيه ومحاسبة المتسببين فيه".

كما تشمل الجرائم السيبرانية عدة أنواع من الهجمات والاختراقات السيبرانية، مثل الاحتيال السيبراني والاختراق السيبراني والهجمات السيبرانية والتجسس السيبراني والإساءة السيبرانية والابتزاز السيبراني وغيرها.

وهو ما سنتطرق إليه في عنوان لاحق بهذه المقالة.

كما تتسم بأنها تهديد خطير للأمن السيبراني والاقتصاد الرقمي في جميع أنحاء العالم، وتتطلب جهودًا كبيرة للحد منها والحفاظ على الأمان والسلامة فيالفضاء السيبراني."

لقد خلف التطور التكنولوجي، وقد أخذت إن الاجرام السيبراني هوأحد النتائج السلبية التي هذه الظاهرة الإجرامية التي فرضت نفسها على المُجتمع، حيزا كبيرا من الدراسات من أجل تحديد مفهومها، حيث نجد أن العديد من الاعمال الاكاديمية حاولت وضع تعريف للجريمة المرتكبة عبر الانترنت، هذه الاخيرة تعد من بين الجرائم التي تباينت تسمياتها عبر المراحل تقنية المعلومات، فقد أُصطلح على تسميتها في بادئ الزمنية لتطورها، والتي إرتبطت بتطور الأمر بإساءة إستخدام الكمبيوتر، ثم جرائم إحتيال الحاسوب، فالجريمة السبيرانية بعدها جرائم الكمبيوتر، والجريمة المُرتبطة بالكمبيوتر، ثم جرائم التقنية العالية إلى جرائم الهاكرز فجرائم الانترنت، وأخيراً جرائم السبيرانية. (مهمل ، 2018)

وتتطلب مواجهة المخاطر السيبرانية، إيجاد التعريف المُناسب، الذي يُحدد التصرفات التي يمكن ان تشكل مصادر حتمية للمخاطر السيبرانية، كتلك المُسيئة والمؤذية، والتي تستتبع بالتالي، تحديد مسؤولية القائمين بها، كما تُحدد السلوك الواجب اتباعه، والذي يُعني عدم الالتزام به، امتناعاً اواهمالاً، ترتب مسؤولية عليه هوالآخر، ويستدعي هذا الأمر بداية، معرفة ماهية الجريمة السيبرانية، التي تُشكل الخطر الاساس الذي تجب مُكافحته، والتعريف ضروري، لكي يتمكن اختصاصي والمعلومات، من تحديد الافعال التي لا بد من تلافي ارتكابها، وتلك التي لا بد من التبليغ عنها، كما يسمح للسلطات المعنية بالمُكافحة، من التحرك على

أساسها بدءاً من اصدار مذكرات التفتيش والتحري، وصولا إلى المصادرة والحجز وجمع الادلة .(الصحيفي، 2020)

كذلك، يمكن تعرف الجريمة السيبرانية، منقبل السلطات القضائية، بتعيين النصوص الملائمة، وايجاد التفسيرات الصحيحة، وللسلطات السياسية، برسم خطوط التعاون مع البلدان الآخر، وان الصعوبة التي تنشأ عن ان بعض الاعمال الجرمية في بلد ما، يمكن الا تكون كذلك، في بلد آخر، ما يستدعي، معالجة خاصة ومُقاربة مُشتركة، من البلدان المعنية، بالتعاون لمُكافحة الجريمة السيبرانية، والحد من تاثيرها على الثقة والأمن، في المجال السيبراني فتعريف الاعمال الجرمية، هوالخطوة الأولى، نحومُكافحتها، والسيطرة عليها.

وانسجاما، مع هذا المنطق، كما مع مبدأ " لا جريمة ولا عقاب دون نص" عمد العديد من البلدان، إلى وضع نصوص قانونية، خاص، بهذا النوع الجديد من الجرائم، التي يمكنها ان تشمل مروحة واسعة من الاعمال غير الشرعية، كتلك التي تستخدم اجهزة الكومبيوتر والشبكات كوسيلة لتنفيذ الجريمة، اوكهدف لها بدءا من عمليات اختراق الأنظمة المعلوماتية وانظمة الاتصالات وصولا إلى الهجمات التي تعطل الخدمات كذلك، تشمل الجريمة السيبرانية، فئة الجرائم التقليدية التي تنفذ عبر المجال السيبراني. الا ان عدم وجود تعريف شامل، اضافة إلى تنوع التعريفات الوطنية، والطبيعة العالمية، للمخاطر وللجريمة، يجعل من الافضل، ان ننطلق من التعريفات التي اعتمدتها، الهيئات والمُنظمات الدولية المُتخصصة، لايجاد المقاييس الخاصة بهذا التعريف وذلك، بالرغم من كونها، تعريفات غير نهائية اوغير مُحددة كفاية، ففي ورشة عمل متخصصة حول المسائل التي تثيرها الجرائم المتصلة بالشبكات، قسمت هذه الجرائم، إلى مجموعتين ضمنت الأولى، حسب المدلول الاضيق، الذي يشير إلى كل

تصرف غير شرعي موجه بالوسائل الإلكترونية، نحوأمن انظمة المعلومات، والبيانات التي تحويها، بينما ضمنت المجموعة الثانية، حسب المدلول الاوسع، كل تصرف غير شرعي يرتكب بواسطة، الأنظمة المعلوماتية، اوبطريقة متصلة بها، ويشمل جرائم كالحيازة غير المشروعة، اوعرض الخدمات وتوزيع المعلومات، بواسطة انظمة معلومات اوشبكات معلومات.(الشهري 2001)

والجريمة السيبرانية هي جريمة تنطوي على استخدام أجهزة الكمبيوتر والإنترنت. ويمكن أن ترتكب ضد فرد أومجموعة من الناس أوالحكومة أوالمنظمات الخاصة. وعادة ما يقصد بها الإضرار بسمعة شخص ما، أوالتسبب في ضرر بدني أوعقلي، أوالاستفادة منه، على سبيل المثال، الفوائد النقدية، ونشر الكراهية والإرهاب، وما إلى ذلك. وكما حدث في عام 1998 أرسلت مجموعة من مقاتلي التاميل، تعرف باسم نمور التاميل، أكثر من 800 رسالة إلكترونية إلى السفارات السريلانكية، وجاء في الرسائل "نحن نمور الإنترنت السود ونحن نفعل ذلك لتعطيل الاتصالات الخاصة بك" حددت سلطات الاستخبارات أنه أول هجوم معروف من قبل الإرهابيين ضد أنظمة الكمبيوتر في بلد ما. (**Tripathi**, 2019)

من جهتها، عمدت الاتفاقية الاوروبية لمُكافحة الجريمة السيبرانية، إلى إيراد ما تعتبره اعمالا غير شرعية تحت عناوين تناولت، الجرائم ضد سرية الأنظمة والبيانات، وسلامتها، وتوفرها والجرائم المتصلة بالاجهزة والجرائم الخاصة بالمحتوى، والجرائم الخاصة بالملكية الفكرية والحقوق المجاورة.

وتعد الجرائم السبيرانية من الجرائم التي تباينت تسمياتها عبر المراحل الزمنية لتطورها، فكانت بداية من مُصطلح إساءة استخدام الكمبيوتر، مرورا بإصطلاح إحتيال الكمبيوتر، والجريمة المعلوماتية، فاصطلاحات جرائم الكمبيوتر، والجريمة

المرتبطة بالكمبيوتر، وجرائم التقنية العالية، إلى جرائم الهاكرز، فجرائم الانترنت إلى آخر المُصطلحات الجرائم السبيرانية.(الصحفي ، 2020)

فمنهم من عرف الجرائم السيبرانية : بأنها "هي التي تتم بواسطة الكمبيوتر ، أوأحد وسائل التقنية الحديثة على كمبيوتر آخر أوأحد وسائل، التقنية الحديثة، مع ضرورة توفر شبكة اتصال فيما بينهما.(الصحفي، 2020)

ولهذا فإننا نجد في كل مرة مع ظهور مُصطلح جديد لجرائم الانترنت يظهر لنا تعريفا جديداً للجريمة السبيرانية، ففقهاء القانون لم يستقروا على تعريف واحد، فنحن لا نستنكر ذلك أبدا لانه من الطبيعي جدا أن يكون هذا الاختلاف، وهذا التنوع في المفاهيم والاراء، وذلك يرجع لحداثة الجرائم السيبرانية، والاختلافات الاثقافات والقوانين بين الدول ، وأيضا خشية في أن يحصروا المُصطلح في نطاق ضيق أومُحدد.(مهمل ، 2018)

ويمكن اعتبار الأمن السيبراني مجموعة من المبادئ التوجيهية والإجراءات المقصودة والمطلوبة لمنع الجريمة السيبرانية، ولكن الأمن السيبراني لا يقتصر على ذلك فحسب. ويختلف نوعا المشاكل اختلافا كبيرا من حيث ما يحدث ومن هم الضحايا، فضلا عن المجالات الأكاديمية التي تدرسهما. ولذلك، يجب النظر إلى الجريمتين، الأمن السيبراني والجرائم السيبرانية، على أنها قضيتان منفصلتان، مع ضمانات مختلفة مصممة لمعالجة مختلف قضايا الخصوصية والأمن لكل منهما. تحتاج جميع أنواع البيانات سواء كانت شخصية أوحكومية أومؤسسية إلى أمان عالي، وبعض البيانات، التي تنتمي إلى نظام الدفاع الحكومي، والبحث العلمي والتطورات، والبنوك، والبحوث الدفاعية وتنظيم التنمية، وما إلى ذلك هي سرية للغاية، وحتى كمية صغيرة من الإهمال لهذه البيانات قد تسبب ضررا كبيرا للأمة

أوالمُجتمع بأسره، وبالتالي، فإن مثل هذه البيانات تحتاج إلى الأمن على مستوى عال جدا. (Tripathi ,2019)

مراحل تطوّر الجريمة السبيرانية:

مرت الجرائم السيبرانية بتطوُّر تاريخي بدأ من إختراع الحاسوب عام 1946، وإنشاء الشبكة العنكبوتية وصولاً إلى الثورة العالمية في الإتصالات والتكنولوجيا، وبحكم هذا التطور تطورت الجريمة بشكل عام والجريمة السيبرانية بشكل خاص ويمكن ملاحظة مراحل تطورها بمايلي :

- **المرحلة الأولى:**

إرتبطت هذه المرحلة بظهور إستخدام الكمبيوتر وربطه بشبكة الانترنت، وكان ذلك في الستينات إلى السبعينات من القرن الماضي، وتميزت هذه المرحلة بعدم الانتسار الواسع الاستخدام تم خلالها رصد عدد قليل من الجرائم بمعدل جريمة واحدة إلى ثلاث جرائم سنوياً ، كما أن طريقة معالجة هذه الجرائم كانت في شكل مقالات صحفية تناقش التلاعب بالبيانات المخزنة، والتدمير الذي يمس انظمة الكمبيوتر والتجسس .(سحواذ، 2015)

- **المرحلة الثانية:**

شهد عقد الثمانينات إرتفاعا نسبيا في معدل الاجرائم السيبراني، حيث ظهر نوع جديد من الجرائم إرتبط بعمليات إقتحام نظم الحاسوب عن بعد ونشر الفيروسات عبر شبكات الكمبيوتر، ما تسبب في تدمير للملفات والبرامج، حيث شاع في هذه الفترة مُصطلح الهاكرز، وهومُصطلح يطلق على مُقتحمي النظم، وتعتبر قضية موريس الشهيرة من بين أهم القضايا المُسجلة عبر الاف في فترة الثمانينات أين تم

نشر فـيروس إلكـتروني عـرف بـدودة مـوريس اجهـزة الكمبيـوتر مـن خـلال الانترنت.(سحواذ، 2015)

- **مرحلة الثالثة:**

شهدت فترة التسعينات تطوراً هائلا في مجال الاجرام السيبراني وتغيـيراً في نطاقهـا ومفهومها حيث أصبحت مواقع الانترنت التسويقية الانشطة أكثر عرضـة لـلـهجمات التي ظهرت بسببها أنماط جديدة مـن الجـرائم، ففـي سـنة 1995 تـم إخـتراق موقـع البيت الابيض الأمريكي، لتليها بعد ذلك العديد من الحـوادث كحادثـة شركـة أوميغـا فيروس وغيرها، ومن أبرز الجرائم في هذه المرحلة قيام صبي بريطاني بإختراق شبكات الحواسيب العسكرية الأمريكية، وكشـف عـن أدق الاتصـالات مـما جعـل المسـؤولين الأمريكيين يصفونه بأنـه أشـد أنـواع إخـتراق أمـن شـبكات الحاسـوب خطـورة هـذا الاختراق على حالة الاستعداد العسكري.(مهمل ، 2018)

- **المرحلة الرابعة:**

وهي الفترة الممتدة مـن سـنة 2000 إلى حـد الان، حيـث واكبهـا تطـورات كثـيرة ومتسارعة مع إرتفاع عدد مستخدمي الانترنت ومعدلات الجرائم بالتبعيـة، وضـخامة الخسائر المالية، وتواصل الجهود الدولية والوطنية لمواجهة هـذه الجـرائم، ففـي عـام 2002 بلغ عدد سـكان العـالم 28، 6 مليـار نسـمة، وعـدد مسـتخدمي الانترنـت 662 مليون مستخدم، ورغم ذلك لم تتفاعل حكومات دول العالم بالقـدر المطلـوب لتـوفير الحماية الازمة من الاجرام السيبراني، بالرغم مـن أنهـا صـارت تعتمـد بشـكل أسـاسي على شبكات الحاسب الآلي في القطاع العـام والخـاص وعـلى مسـتوى الافـراد، وبعـد الهجمات الإلكترونيـة الشـهيرة عـلى دولـة إسـتونيا عـام 2007 ، إنتبهـت الكثـير مـن

الـدول لهـذا الخطـر الـذي يـدمر البنيـات التحتيـة للمعلومـات وتقنيـة الاتصـالات والشبكات، ويعطـل كـل المرافـق الحيويـة، فبـدأت الـدول التفكـير بجديـة في إعـداد إستراتيجيات للامن السيبراني .(بلعزوق، 2017)

أسباب الجرائم السيبرانية:

للجريمة السبيرانية اساب عدة والدافع أوالباعث هوالعامل المحرك للارادة الـذي يوجه الســلوك الإجرامي كالمحبة والشـفقة والبغضـاء والانتقـام فهوعبـارة عـن قـوة نفسية تدفع الارداة إلى الاتجـاهً المخـالف للنـاس، كـام أنـه نحوارتكـاب الجريمـــة؛ وهويختلف من جريمة إلى أخرى تبعا للختلاف بالنسبة للجريمة الواحدة مـن شـخص لاخر، وترتكب الجرائم السـيبيرانية بـدوافع متنوعـه ومنتظمـة، ومـن هـذه الأسـباب مايلي:

أ. الرغبة في جمع المعلومات وتعلمها.

ب. الاستيلاء على المعلومات.

ت. الرغبة في قهر النظام والتفوق عىل تعقيد الوسائل التقنية.

ث. الحاق الضرر بأشخاص أوجهات بعينها، على صورة ابتزاز أوتهديد أوتشهير.

ج. السعي وراء الربح، كاستخدام شبكة الانترنت في الاتجار بالبشر.

ح. تهديد الأمن القومي والعســكري، كحرب المعلومات والتجسس الإلكتروني.

خصائص الجريمة السيبرانية:

تتميز الجريمة السيبرانية بعدة خصائص منها:(الصحفي، 2020)

1. تتميزالجـرائم التقنيــة بخصـائص تختلـف إلى حـد ما عن الجريمة العادية على النحوالتالي:

2. جرائم عابرة للدول: وهي الجرائم التي تقع بين اكثر من دولة ولا تعترف بالحدود الجغرافية مثلها مثل جرائم غسيل الأموال والمخدرات وغيرها. ففي عصر الحاسوب والانترنت أمكن ربط اعداد هائلة من الحواسيب عبر العالم، وعند وقوع جريمة الكترونية غالبا يكون الجاني في بلد والمجني عليه في بلد آخر كما قد يكون الضرر في بلد ثالث.

3. جرائم مغرية للمرتكبين: ان سرعة تنفيذها (كبسة زر) وامكانية القيام بها عن بعد دون اشتراط التواجد في مسرح الجريمة تجعلها مغرية بما لايقبل الشك.

4. جرائم سهلة الارتكاب: فهي جرائم ناعمة، واطلق عليها البعض اسم جرائم الياقات البيضاء. وعند توفر التقنية اللازمة للجاني يصبح ارتكاب الجريمة من السهولة بمكان ولا تحتاج إلى وقت ولا جهد..

5. جرائم سريعة التنفيذ: فسرعة ارتكاب الجريمة قد تكون خلال جزء من الثانية، وقد لا تتطلب الاعداد والتخطيط قبل التنفيذ .

6. جرائم عن بُعد: فيمكن للجاني تنفيذ جريمته وهوفي دولة بعيدة، عن دولته .

7. جرائم عابرة للحدود: فهي لا تعرف الحدود الجغرافية للدول، وارتباط العالم بشبكة واحدة، وهذا قد يسبب إشكاليات لدى الاختصاص القضائي من حيث التحقيق والمحاكمة، وذلك تبعا لتعقيد الاجراءات التي تحكمها الاتفاقيات والمعاهدات والعلاقات الدولية، والتنازع فيما بينهما على أي القانون الواجب التطبيق.

8. جرائم صعبة الإثبات: يستخدم الجاني في هذه الجرائم وسائل فنية معقدة وسريعة في كثير من الأحيان قد لا تستغرق أكثر من بضع ثواني، بالإضافة إلى سهولة محوالدليل والتلاعب فيه والأهم عدم تقبل القضاء في الكثير من الدول

للأدلة التقنية المعلوماتية التي تتكون من دوائر وحقول مغناطيسية ونبضات كهربائية غير ملموسة بالحواس الطبيعية للإنسان.

وتكمن صعوبة إثباتها إلى أن متابعتها واكتشافها عن طريق الصدفة، ومن الصعوبة حصرها في مكان معين، حيث أنها لا تترك أثراً واضحا للعيان، أوتشاهد بالعين المجردة، فما هي الا أرقام تدور في السجلات والمواقع الإلكترونية، كما أن الجرائم التي لم تكتشف هي أكثر بكثير من تلك التي كشف عنها وتعود الصعوبة لعدة أسباب هي: (القرعان، 2017)

أ. إنها كجريمة لا تترك أثراً بعد ارتكابها .

ب. صعوبة الاحتفاظ الفني بآثارها إن وجدت .

ت. تحتاج لخبرة فنية يصعب على المُحقق التقليدي التعامل معها .

ث. تعتمد على الخداع في ارتكابها، والتضبيب في التعريف على مُرتكبيها .

ج. تعتمد على مستوى من الذكاء المرتفع في ارتكابها .

ح. جرائم ناعمة: فهي جرائم لا تمارس بالعنف، ولاتحتاج إلى أدني مجهود عضلي بعكس بعض الجرائم التقليدية

ومن هنا فاننا نلاحظ بأن المُجرم السيبراني يتميز بمهارات عالية، فهويعتمد على قدراته العقلية بالذكاء والدهاء ومعرفة الطرق السيبرانية اتلاف البرامج واختراق الحواجز الأمنية، ولعل الدافع للمجرمين السيبرانيين قد يكون بدافع المال بلجوئهم إلى الطرق الغير مشروعة وذلك بسبب ما يعانوه من البطالة، وقد يكون بدوافع عقائدية وسياسية، وقد يكون بدوافع شخصية كقيام الموظف بالانتقام من المؤسسة أوالشركة التي قامت بفصله، أوللتجسس وانتهاك الخصوصية.

والمبدأ الرئيسي لقانون الجـرائم السـيبرانية هومعاقبـة الوصـول غـير المصرح بـه أوالاستخدام غير القانوني لأنظمة الكمبيوتر والإنترنـت بنوايـا إجراميـة، بحيـث يمكـن منع تلف وتغيير الأنظمة والبيانات المتعلقة بها ومع ذلك، فإن أكـبر تهديـد للجـرائم السيبرانية هوعلى الأمن المالي للفرد وكذلك الحكومة.

أنواع الجرائم السيبرانية:

هناك عدة جرائم تنطوي تحت مظلة الجرائم السبيرانية هي الاتية:

أولا: جرائم التعدي على البيانات المعلوماتية:

تشمل الجرائم التـي يكـون موضـوعها البيانـات المعلوماتيـة، أي التـي تقـع عـلى بيانات معلوماتية، وهي جرائم التعرض للبيانات المعلوماتية، وجرائم اعتراض بيانـات معلوماتية، والبيانات هي كل ما يمكـن تخزينـه ومُعالجتـه وتوليـده ونقلـه بواسـطة الحاسب الآلي، كالأرقام والحروف والرموز وما إلى ذلك.(بن داود ، 2020)

ثانيا: جرائم التعدي على الأنظمة المعلوماتية:

تشمل جرائم الولوج غير المشرع إلى نظام معلوماتي أوالمكوث فيـه، مـع التعـرض للبيانات المعلوماتيـة وجـرائم إعاقـة عمـل معلومـاتي، ويتمثـل النظـام المعلومـاتي في مجموعة البرامج وأدوات مُعدة لمُعالجة وإدارة البيانات والمعلومات.

ثالثا: إساءة استعمال الأجهزة أوالبرامج المعلوماتية: (القحطاني ، 2016)

تتضمن هذه الجرائم كل من قدم أوأنتج أووزع أوحاز بغـرض الاسـتخدام جهـازا أوبرنامجا معلوماتيـا أوأي بيانـات معلوماتيـة معـدة أوكلـمات سر أوكـودات دخـول، وذلك بغرض اقتراف أي من الجرائم المنصوص عليها سابقا.

ويتضمن البرنامج المعلوماتي مجموعة من التعليمات والأوامر القابلة للتنفيذ باستخدام الحاسب الآلي ومعدة لإنجاز مهمة ما، إما البرامج المعلوماتية هي الكيان المعنوي غير المادي من برامج ومعلومات وما إليها ليكون قادرا على القيام بوظيفة.

رابعا: الجرائم الواقعة على الأموال: (القحطاني، 2016)

أ. جرم الاحتيال أوالغش بوسيلة معلوماتية.

ب. جرم التزوير المعلوماتي.

ت. جرم الاختلاس أوسرقة أموال بوسيلة معلوماتية.

ث. جرم أعمال التسويق والترويج غير المرغوب فيها

ج. جرم الاستيلاء على أدوات التعريف والهوية المُستخدمة في نظام معلوماتي، والاستخدام غير المشرع لها.

ح. جرم الاطلاع على معلومات سرية، أوحساسة أوإفشائها.

خامسا: جرائم الاستغلال الجنسي للقاصرات:

هي الجرائم التي تظهرها الأفعال التي تتعلق باستغلال القاصرين في أعمال جنسية، والاتجار بهم وتشمل:(بن داود، 2020)

1) الرسومات أوالصور أوالكتابات أوالأفلام أوالإشارات.

2) أعمال إباحية يشارك فيها القاصرون.

3) تتعلق باستغلال القاصرين في المواد الإباحية.

4) إنتاج مواد إباحية للقاصرين بقصد بثها بواسطة نظام معلوماتي.

سادسا: جرائم التعدي على الملكية الفكرية للأعمال الرقمية:

تشمل جرام وضع اسم مختلس على عمل، وجرم تقليد إمضاء المؤلف أوختمه، وجرم تقليد عمل رقمي أوقرصنة البرمجيات، وجرم بيع أوعرض عمل مقلد أووضعه في التداول، وجرم الاعتداء على أي حق من حقوق المؤلف أوالحقوق المجاورة.

سابعا: جرائم البطاقات المصرفية والنقود الإلكترونية:

تشمل أعمال تقليد بطاقات مصرفية بصورة غير مشروعة واستعمالها عن قصد، وتزوير إلكترونية بصورة غير مشروعة عن قصد، لما لذلك من إخلال بالاقتصاد الوطني وتأثير سلبي على العمليات المصرفية.

ثامنا: الجرائم التي تمس المعلومات الشخصية:

تتضمن الأفعال الجرمية التي تتعلق بمعالجة البيانات ذات الطابع الشخصي دون حيازة تصريح أوترخيص مسبق يتيح القيام بالمُعالجة، وإنشاء معلومات ذات طابع شخصي لأشخاص لا يحق لهم الاطلاع عليها.

تاسعا: جرائم العنصرية والجرائم ضد الإنسانية بوسائل معلوماتية: (بن داود، 2020)

1. جرم نشر وتوزيع المعلومات العنصرية بوسائل معلوماتية.
2. جرم تهديد أشخاص، أوالتعدي عليهم بسبب انتهائهم العرقي أوالمذهبي، أولونهم وذلك بوسائل معلوماتية.
3. جرم توزيع معلومات بوسيلة إلكترونية من شانها إنكار، أوتشويه أوتبرير أعمال إبادة جماعية أوجرائم ضد الإنسانية.
4. جرم المُساعدة أوالتحريض بوسيلة إلكترونية على ارتكاب جرائم ضد الإنسانية.

عاشراً: جرائم المقامرة وترويج المواد المخدرة بوسائل معلوماتية عبر الإنترنت:

وتشمل جرم تملك وإدارة مشروع مقامرة، وجرم تسهيل وتشجيع مشروع مقامرة، وجرم ترويج الكحول للقاصرين وجرم ترويج المواد المُخدرة.

حادي عشر: الجرائم المعلوماتية ضد الدولة والسلامة العامة:

تتضمن الأفعال الجرمية الناشئة عن المعلوماتية التي تطال الدولة وسامتها وأمنها، واستقرارها ونظامها القانوني، وهي: (القحطاني ، 2016)

أ. جرائم تعطيل الأعمال الحكومية أوأعمال السلطة العامة باستعمال وسيلة معلوماتية.

ب. جرائم الإخفاق في الإبلاغ أوالإبلاغ عن قصد بشكل خاطئ عن جرائم المعلوماتية، والاطلاع أوالحصول على معلومات سرية تخص الدولة.

وذلك من خلال شبكة الإنترنت أوباستعمال وسيلة معلوماتية، بالإضافة إلى فعل العبث بالأدلة القضائية المعلوماتية أوإتلافها أوإخفائها، والأعمال الإرهابية التي ترتكب باستخدام شبكة الإنترنت أوأي وسيلة معلوماتية، وجرائم التحريض على القتل عبر الإنترنت أوأيه وسيلة معلوماتية.

ثاني عشر: جرائم تشفير المعلومات:

تشمل أفعال تسويق أوتوزيع أوتصدير أواستيراد وسائل تشفير، بالإضافة إلى أفعال تقديم وسائل تشفير تؤمن السرية دون حيازة تصريح أوترخيص من قبل المراجع الرسمية المُختصة في الدولة، وأيضا بيع أوتسويق أوتأجير وسائل تشفير ممنوعة. (القحطاني ، 2016)

تكلفة الجريمة السيبرانية:

من الصعب قياس تكاليف الجريمة السيبرانية، ولكنها بـأي معيـار معقـول كبـيرة وتنموأضعافا مضاعفة ويجمع المعهد المعنـي بـأمن الحاسـوب سـنويا أشـمل مصـدر متاح للبيانات عن التكاليف، بمشاركة المعهـد بيـتر نيومـان، "محـن ومخـاطر نظـام المعلومات"، وفي أوائل عام 2000، كان نحو210 بلدان متصلا بشـبكة الإنترنـت، التـي كان عدد مستخدميها حوالي 300 مليـون مسـتخدم، وجـرى في عـام 2000 ربـط 210 بلدان بشبكة الإنترنت، بلغ عدد مستخدميها نحو300 مليون مستخدم؛ و200 مليـون مستخدم، ومن المتوقع أن يرتفع عدد المستخدمين إلى بليون مستخدم في عام 2005.، والتي كانت متاحة ، وقد يثبت أن خروقات أمن الكمبيوتر واسعة النطـاق ومتنوعـة ومُكلفة، ويستثمر المجيبون بكثافة في مجموعة متنوعـة مـن التكنولوجيـات الأمنيـة، بتكلفة تقدرها المؤسسة الدولية للبيانات بأنها تنمومن بليوني دولار في عام 1999 إلى 7.4 بلايين دولار في عام (**Goodman, & Sofaer** 2000,)

ويتعين إضافة تكاليف التـأمين ضـد الجـرائم السـيبرانية إلى هـذه المبـالغ، وهـي تغطية جديدة لسوق آخذة في التوسع ، أما الذين لم يشهدوا مثل هذه الأحداث فقد انخفضوا من 37 % إلى 18 % في الفترة نفسها 37% فقط من جميع الهجمات المبلغ عنها في عام 1996 شـملت اتصـالات بالإنترنـت؛ و30 % فقـط مـن جميـع الهجـمات المبلـغ عنهـا في عـام 1996 كانـت تتعلـق باتصـالات بالإنترنـت؛ و30 % مـن جميـع الهجمات التي تم الإبلاغ عنها وفي عام 2000، ارتفعـت هـذه النسـبة إلى 59 %، مـع انخفاض مماثل في الهجمات الداخليـة حتـى الآن، وكانـت الفئـة الأكـثر خطـورة مـن الخسائر الماليـة المبلـغ عنهـا مـن خـلال سرقـة المعلومـات الخاصـة، والتـي يبـدوأنها تشمل الهجمات التي تؤدي إلى سرقة البيانـات الماليـة، وتشـمل الفئـات الأخـرى مـن

الخسائر الكبيرة الاحتيال، وهجمات الفيروسات والحرمان من الخدمة، والتخريب، وتقدير الأضرار النقدية التي تسببها الجريمة السيبرانية على المستوى التقني البحث إنقسم جميع الرسائل على الإنترنت إلى "رزم تفصل وتتنقل عبر أجهزة التوجيه والخوادم المتاحة الموجودة في جميع أنحاء العالم، وتشمل نقاط الضعف هذه ما يلي: (**Goodman , & Sofaer** 2000,)

أ. مجموعة مُستهدفة من أجهزة الكمبيوتر والمُستخدمين في جميع أنحاء العالم للإيذاء، أوللاستغلال في الحرمان من الخدمة أوغيرها من الهجمات، مما يمكن المهاجمين من إحداث المزيد من الضرر دون بذل أي جهد أكثر مما قد يكون ضروريا في مهاجمة أجهزة الكمبيوتر أوالمستخدمين في حالة واحدة.

ب. وجود مجموعة من الأجهزة المحمولة والمُستخدمين المُستهدفين في جميع أنحاء العالم، بما في ذلك الهجمات التي قد تكون ضرورية في مُهاجمة أجهزة الكمبيوتر أوالمُستخدمين في حالة واحدة.

ت. وجود مجموعة مُستهدفة من أجهزة الكمبيوتر والمُستخدمين على نطاق العالم للإيذاء أوالاستغلال في حالات الحرمان من الخدمة أوغيرها من الهجمات، مما يمكن المهاجمين من إحداث ضرر أكبر دون بذل أي جهد أكثر مما قد يكون ضروريا في مهاجمة أجهزة الكمبيوتر أوالمُستخدمين في حالة واحدة.

ث. وجود مجموعة مستهدفة من أجهزة الكمبيوتر والمستخدمين على نطاق العالم، أواستغلالها.

ج. التفاوتات الواسعة الانتشار بين الدول، في البيئة القانونية أوالتنظيمية، أوالسياساتية المتعلقة بالجرائم السيبرانية.

ح. درجة عالية من التعاون الدولي في مُلاحقة هذه الجرائم وردعها، وكانت أكثر الهجمات السيبرانية ضررا حتى الآن عابرة للحدود الوطنية، نشأت في العديد من البلدان المختلفة واستهدفت الحواسيب في كل مكان.

صور الجريمة السيبرانية في الفقه الجنائي:

إذا بحثنا في تصنيف الفقهاء للجريمة السيبرانية، نجد أن البعض منهم يقسمها إلى جرائم تستهدف نظام المعلومات وأخرى ترتكب بواسطته، والبعض الاخر يصنفها إستنادا إلى الاسلوب المتبع في الجريمة، وآخرون يستندون إلى الباعث أوالدافع إلرتكاب الجريمة، وغيرهم يؤسس تقسيمه على تهديد محل الاعتداء، وكذا تعدد الحق المعتدى عليه، وكلها تصنيفات ودراسات رافقت موجات التشريع في ميدان تقنية المعلومات وعكست التطور التاريخي لهذه الظاهرة الإجرامية، ، ولا نبالغ إن قلنا إن ثمة نظريات ومعايير لتصنيف طوائف جرائم تقنية المعلومات الحديثة بعدد المؤلفين والباحثين في هذا المجال القانوني. (جعفر، 2013)

وللجريمة السبيرانية صور عدة تتمثل فيما يلي : (الزرفي، 2019)

1. **الاعتداء السيبراني على معطيات الحاسب الآلي:**

يتمثل الاعتداء السبيراني كـإتلاف البيانات والمعلومات والبرامج، والتلاعب بالمعلومات المخزنة داخل الحاسب .

2. **الاعتداء السيبراني على حرمة الحياة الخاصة، وتتمثل فيما يلي: (الزرفي، 2019)**

أ. يكون بالإفشاء والنشر العلني للوقائع الخاصة التي تمس الشخص كإفشاء واقعة إصابته بمرض مخزي، أو عجز عن سداد ديونه أو نشر صورة البنه.

ب. تشويه سمعة الشخص في نظر الجمهور، والتشهير به.

ت. الاستيلاء على بعض العناصر الشخصية كالاسم والصورة والبيانات الشخصية المتصلة بالحياة الخاصة.

3. الاعتداء السيبراني على حقوق الملكية الفكرية :

ويكون بالاعتداء على العلامات التجارية وبراءات الاختراع، وكذلك نسخ وتقليد البرمج، واعادة إنتاجها وصنعها دون ترخيص فهواعتداء على الحقوق المالية والحقوق الأدبية.

4. الاستيلاء والنصب والاحتيال السيبراني. (الشمري، 2016)

ويتمثل هذا الاحتيال اما لنفسه، أولغيره على مال منقول أوعلى سند، أوتوقيع هذا السند، وذلك عن طريق الاحتيال، أواتخاذ اسم كاذب، أوانتحال صفة غير صحيحة .

5. الانتحال والتغرير السيبراني (الشمري، 2016)

أ. انتحال شخصية فردية: بسبب التنامي المتزايد لشبكة الانترنت والذي أعطى للمجرمين قدرة أكبر على جمع المعلومات للشخصية المطلوبة والانترنت منها في ارتكاب جرائمهم فتنتشر في شبكة الانترنت الكثير من الاعلانات المشبوهة والتي تحاكي الطمع الانساني في محاولة الاستيلاء على معلومات اختيارية من الضحية، فهناك اعلان عن جائزة فخمة يكسبها من يساهم بمبلغ رمزي لجهة خيرية، وهذا يتطلب الافصاح عن معلومات سرية الأمر الذي يؤدي إلى الاستيلاء على الرصيد البنكي ، أوالسحب من البطاقة الائتمانية أوالاساءة إلى سمعة الضحية.

ب. إنتحال شخصية المواقع : ويكــون باختــراق حاجز أمني وتتــم عمليــة الانتحــال بهجوم يشــنه المجرم على الموقع للسيطرة عليه ومن ثم يقــوم بتحويلــه كموقــع بيني أويحاول المجرم اختراق موقع ألحد مقدمي الخدمة المشـــهورين ثــم يقــوم بتركيب البرنامــج الخــاص به هنــاك مما يؤدي إلى توجه أي شــخص إلى موقعه بمجرد كتابة اسم الموقع المشهور.

6. **الإبتزاز والتهديد السيبراني :**

يتمثل الابتزاز والتهديد السبيراني نشر الصور أومعلومات صحيحة ، أوغير صحيحة عن المجني عليه بهدف الحصول على المال أوعلاقة غير مشروعة .

7. **التنصت السيبراني :**

يتمثل التنصت السبيراني باســتخدام برنامــج فــي جهــاز الشــخص المُعتــدى عليه، حيث يتمكن من خلاله الاطلاع والاستماع إلى جميــع المُحادثــات والمراسـلات الصــادرة مــن الشــخص المعتــدى عليــه ويـتم إدخــال هـذا الملـف إلى جهـاز المعتدى عليه عن طريق البريد الإلكـتروني ، أوعـن طريــق مواقــع مغريـة يزورهــا المعتــدى عليــه فيقــوم بتنزيــل بعض البرامج ومنهـا برنـامج التنصـت، اســتخدام برنامــج المحادثــة، فيقوم المجــرم بإغــراء الضحيــة بــأن هــذا البرنامــج يحتـوي علــى ألعاب مثيرة أوغير ذلــك فيقــوم الضحية باســتقبال الملف.

وجريمــة التنصـت إمـا أن تكـون بالتقـاط وهومشـاهدة البيانـات عـبر الشـبكة المعلوماتية، أوأحد أجهزة الحاسب أوأن تكون بالاعتراض ، وهـواعتراض مـا هومرسـل عبر الشبكة المعلوماتية، أوأحــد أجهــزة الحاســب الآلي بحيــث يتــم عمــل إجرام كتحويل أموال مثلاً.

8. السطو السيبراني على أموال البنوك :

يتم السطوعن طريق استخدام الجاني للحاسب الآلي للدخول إلى شبكة الانترنت والوصول غير المشروع إلى البنوك والمصارف والمؤسسات المالية، وتحويل الأموال من تلك الحسابات الخاصة بالعملاء إلى حسابات أخرى وذلك بإدخال بيانات غير حقيقية أوتعديل أومسح البيانات الموجودة بقصد اختلاس الأموال أونقلها، واتلافها وتقوم هذه التقنية على الاستيلاء على الأموال بكميات صغيرة جداً من الحسابات الكبيرة بحيث ال يالحظ نقصان هذه الأموال .

9. الاعتداء السيبراني على الاخلاق والاتجار بالبشر وبالمخدرات وذلك من خلال مايلي : (الصحفي، 2020)

أ- إنشاء موقع على الشبكة المعلوماتية أوأحد أجهزة الحاسب الآلي ، أونشره للإلتجار في الجنس البشري ، أوتسهيل التعامل به.

ب- إنشاء المواد والبيانات المُتعلقة بالشبكات الاباحية أوأنشطة الميسر المُخلة بالاداب العامة أونشرها ، أوترويجها.

ت- إنشاء موقع على الشبكة المعلوماتية أوأحد أجهزة الحاسب الآلي أونشره للاتجار بالمخدرات أوالمؤثرات العقلية، أوترويجها أوطرائق تعاطيها أوتسهيل التعامل بها .

10. الاعتداء السيبراني على الأمن:

يتمثل الاعتداء السبيراني على الأمن، بإنشاء موقع لمنظمات إرهابية على الشبكة المعلوماتية، أوأحد أجهزة الحاسب الآلي أونشره لتسهيل الاتصال بقيادات تلك المنظمات، أوأي من أعضائها أوترويج أفكارها أوتمويلها ، أونشر كيفية تصنيع الاجهزة الحارقة أوالمُتفجرات، أوأي أداة تستخدم في الاعمال الارهابية،

والدخول غير المشـروع إلى موقع إلكتروني أونظـام معلومـاتي مبـاشرة أوعـن طريـق الشبكة المعلوماتيـة أوأحـد أجهـزة الحاسـب الآلي للحصـول عـلى بيانـات تمـس الأمن الداخلي، أوالخارجي للدولة أواقتصادها الوطن.(الصحفي، 2020)

الفرق بين الجريمة السيبيرانية وغيرها من الجرائم:

توجد فروق بين الجريمـة المعلوماتيـة والجريمـة الإلكترونيـة، فمـن حيـث مسرح الجريمة "الوقائع" غير موجود بل هوالفضاء السبيراني والفضاء الإلكتروني، وأما الجـاني والمجني عليه لا يشـرط أن يكون في مكـان واحـد أوفي دولـة واحـدة عـل عكـس الحال في الجرائم العادية، كالمخدرات مثلا التي لها مسرح جريمة، ومن ثم يكـون لهـا محل معاينة، اما مبـدأ إقليمية النص الجنائي، وما يعنيه ذلـك للجرائـم المعلوماتيـة أوالإلكترونيـة قابلـة للتوسـع والابتكـار، إذ هـي مرتبطـة في الاسـاس بالتقـدم التقنـي والمعلومات.(الردفاني ، 2014)

وهنـاك جوانـب معينـة يمكـن التمييـز حولهـا بـين الجريمـة السـيبرانية والأمـن السيبراني، وهي: (**Tripathi**, 2019)

أ. أنواع الجرائم: في الأمن السيبراني، وأنواع الجرائم حيث برامج الكمبيوتر أوالأجهزة أوشبكة الكمبيوتر، هوالهدف الرئيسي ، كانتزاع الفديـة، والفيروسـات، والديـدان، وتوزيع هجمات الحرمان من الخدمة .

ب. في الجرائم السيبرانية، تكون الجرائم هي المكان الذي يكون فيه الفرد أومجموعة من الأفراد وبياناتهم هي الهدف الرئيسي، ويمكن أن تكون الحكومات والمنظمات أيضا هدفا للجرائم السيبرانية (اعمال البلطجـة الإلكترونيـة، وخطـاب الكراهيـة، والاتجار بالمواد الإباحية للأطفال، والتصيد).

ت. الضحايا: يختلف الضحايا في هذين المجالين أيضا، وفي مجال الأمن السيبراني، يكون الضحايا حكومات وشركات، في حين أن نطاق الضحايا في الجرائم السيبرانية واسع إلى حد ما لأن الضحايا يمكن أن يمتدوا من الأفراد والأسر، والمنظمات والحكومات والشركات.

ث. مجال الدراسة: يدرس هذان المجالان في مجالات مختلفة.

ج. يتم التعامل مع الأمن السيبراني في إطار علوم الكمبيوتر وهندسة الكمبيوتر وتكنولوجيا المعلومات.

ح. تستخدم استراتيجيات الترميز والشبكات والهندسة لجعل الشبكات أكثر أمانا.

خ. من ناحية أخرى، يتم التعامل مع الجرائم السيبرانية في ظل علم الجريمة وعلم النفس وعلم الاجتماع. أساسا، هوالفهم النظري لكيفية وسبب ارتكاب الجريمة وكيف يمكن منعها.

الجرائم السيبرانية الاكثر انتشارا عام 2022:

عام 2022، زادت الضربات التي نفذتها عصابات اختراق عالمية ومحلية في مختلف الدول بأهداف وأغراض متباينة منها السياسي ومنها الاقتصادي هذا وقد ابلغت وكالة الأمن السيبراني وأمن البنية التحتية الأمريكية (**CISA**) عن زيادة هائلة بنسبة 62 ٪ سنويًا في قضايا الجرائم الإلكترونية بين فبراير 2021 وفبراير 2022، وبشكل عام، توجد 3 مستجدات واستحداثات عندما يتعلق الأمر بالجرائم السيبرانية في عام 2022 مقارنة بالسنوات السابقة وهي :

أولا: التركيز الكبير على العملات المشفرة.

ثانيا: المزيد من الهجمات الموزعة على الشركات الصغيرة.

ثالثا: زيادة التنوع في عمليات الاحتيال لسرقة الهوية.

ورغم أن الأمر قد يكون تحت السيطرة مع تعاظم القدرة على مواجهة تلك الهجمات، إلا أنه ومع ذلك زادت فرصة مجرمي الإنترنت للعثور على الأهداف غير المحصنة واستغلالها مع التحول إلى العمل عبر الإنترنت، لذا يجب على الصناعة التقنية التعجيل بالأمن السيبراني وتحسينه بشكل عام، هذا وتتنوع الجرائم الإلكترونية، حيث يمكن للجرائم الإلكترونية المالية سرقة الأموال منك مباشرةً. يمكن أيضا استخدام معلوماتك الشخصية والتجارية لسرقة الأموال. يمكن أن تشمل الجرائم الإلكترونية أيضا التجسس الصناعي، حيث يسرق مجرموالإنترنت الأفكار وبراءات الاختراع وحتى العملاء، وحسب ما اورد موقع "**techgenix**" فان اكثر انواع الجرائم السيبرانية شيوعا عام 2022 هي:

1- **التصيد الاحتيالي:**

يتضمن التصيد الاحتيالي استخدام رسائل بريد إلكتروني أوصفحات ويب جديرة بالثقة لخداع الأشخاص من أجل النقر فوق الارتباط أوتقديم معلوماتهم الشخصية، وتسمح هجمات التصيد الاحتيالي الناجحة لمجرمي الإنترنت بسرقة أموالك أوهويتك.

مع برامج الأمان والمعرفة الحالية، يكون معدل نجاح هجمات التصيد الاحتيالي منخفضًا بشكل لا يصدق، ولكن مع وجود أكثر من 100 مليون هجوم يوميًا، فلا عجب أن يتمكن بعض المهاجمين من الوصول إلى أهدافهم، حتى الشركات الكبيرة يمكن أن تتأثر.

2- الاحتيال الهاتفي:

هذا النوع يوصف بأنه أحد أقدم الحيل في جرائم التصيد الاحتيالي، هوشكل شائع آخر يتم من خلال المكالمات بدلاً من النصوص المكتوبة. وكان شائعًا ضد البنوك منذ ما يقرب من عقدين من الزمن عندما كانت الخدمات المصرفية الإلكترونية قد بدأت للتو. والآن ازدهر بقوة مع انتشار التجارة الإلكترونية، وينتحل المتصل صفة علامات تجارية أووكالات حكومية شرعية وقد يطلب معلومات حساسة مثل تفاصيل الحساب المصرفي أوالأموال، سواء من خلال التحويل الإلكتروني أوبطاقات الهدايا، ومع ذلك، في حين أن هذه الأنواع من العمليات لا تزال موجودة في الوقت الحالي، فقد تطور المحتالون ووجدوا طريقة أكثر فاعلية. على سبيل المثال، قد يدعم المهاجمون في هجوم تصيد احتيالي معقد بريدًا إلكترونيًا مزيفًا مع مكالمة تصيد كمتابعة لإضافة شرعية إلى السيناريوالذي أعدوه.

3- رفض الخدمات الموزعة:

هذا النوع من الهجمات الإلكترونية يعتبر بسيطا إلى حد ما، ولهذا السبب يستخدمه العديد من مجرمي الإنترنت، وهي جريمة إلكترونية يقوم فيها المهاجم بإغراق الخادم بحركة مرور الإنترنت لمنع المستخدمين من الوصول إلى الخدمات والمواقع المتصلة عبر الإنترنت، حيث تستخدم هجمات **DDoS** الآلاف من حسابات الروبوت للوصول إلى صفحة الويب في نفس الوقت، وبالتالي رفض الوصول إلى الآخرين وحتى إيقاف موقع الويب، وعلى الرغم من أن هذه الهجمات لا تسرق بياناتك أوتخترق شبكتك، إلا أنها تؤثر على قاعدة البيانات الكاملة للشركة عبر الإنترنت. يمكن أن تكون أيضا ستارًا دخانيًا لخرق البيانات أوهجوم الفدية، وأدى تطوير معالجات جديدة وزيادة الاتصال البيني على الويب المظلم إلى جعل

بـدء هجـمات **DDoS** أسـهل بكثـير. يمكـن للمعـالج المتطـور بـدء تشـغيل آلاف التطبيقات ذاتية التنفيذ (الروبوتات)، وقد أبلغت ثلاثـة أربـاع الشركـات تقريبًـا عـن هجمات **DDoS** في عام 2020. وفي عام 2022، يبدوأن الـرقم لـن يـنخفض. ولحسـن الحظ، تم إيقاف معظم الهجمات لأن جميع أنظمة تشغيل الخوادم الجديدة تقريبًـا لديها إجراءات وقائية.

4- سرقة الهوية:

يسرق مجرموالإنترنت هويتك لاستخدام معلوماتك الخاصـة واسـمك للوصـول إلى خدمات أوسلع مختلفة، حيث يمكن لأي شخص لديـه معلومـات بطاقتـك الائتمانيـة استخدامها لشراء أشياء أوإرسال أموال إلى الخارج، وتحدث سرقة الهوية بشكل شـائع عندما يشارك الضحايا معلوماتهم عبر وسائل التواصل الاجتماعـي أوهجـمات التصـيد الاحتيالي، وإذا أصبحت الشركة التي تخزن معلوماتك ضحية لهجوم إلكتروني، فـيمكن أيضا سرقة هويتك، هذا وقد ونشرت المنظمات، مثل جمعية المصرفيين الكندية، دليلًا حول كيفية اكتشاف عمليات الاحتيال لسرقة الهوية. ولسوء الحظ، فإن زيادة الـوعي هي الطريقة الوحيدة للبقاء في مأمن من سرقة الهوية.

5- هجمات برامج الفدية:

تحدث هجمات بـرامج الفديـة عنـدما تكـون بالفعـل ضحية للتصيّد الاحتيـالي أوالتصـيّد الهـاتفي أوالرسـائل الإلكترونيـة الخادعـة، حيـث يأخـذ المجرمـون بياناتـك الحساسة ويحتفظون بها حتى تدفع، وغالبًا ما تسـتخدم الهجـمات الإلكترونيـة عـدة طرق معاً، وبمجرد النقر فوق رابط التصيد، قد يبدأ تنزيل ملف الاخـتراق، حيـث قـد يخـدعك الـرابط للكشـف عـن معلوماتـك الخاصـة. وبعـد ذلـك باسـتخدام هـذه

المعلومات يمكن لمجرمي الإنترنت الوصول إلى نظامك وتنزيل ملفاتك الشخصية والتجارية، وقد يحتفظ مجرموالإنترنت أيضا بمعلوماتك للحصول على فدية أوتغيير كلمات المرور وإبقاء نظامك بأكمله في حالة فدية. ولم تعد الأهداف هي الشركات الضخمة التي لديها سرعة في الدفع فقط، بل يتم الآن الهجوم على الشركات الصغيرة وحتى الأفراد أيضا. (مقال منشور، الوطن/ ارم نيوز، البحرين، 2022)

المبحث الثاني: المجرم السيبراني اصنافه ومميزاته واساليبه.

المجرم السيبراني:

هومُجرم يتمتع بقدرة فائقة من الذكاء إذ يستغل مهاراته في اختراق الشبكات وكسر الشفرات وكلمات المرور موظفا مهاراته تخزين البيانات والمعلومات والتحكم في أنظمة الشبكات، كما أنهم في الغالب يتميزون بأنهم أفراد ذوي مكانة في المجتمع من أصحاب الوظائف الحيوية سواء في القطاع الخاص أوفي القطاع العام، وقد أطلق عليهم مصطلح ذوي الياقات البيضاء.

وقد ثبت من خلال الدراسات النفسية للمُجرم السيبراني بأن ليس لديه أي شعور بعدم مشروعية الافعال التي يمارسها، وعدم استحقاقه للعقاب، كما تغيب مشاعر الاحساس بالذنب، وذلك لربما عدم احتكاك الجاني المجرم بالمجني عليه مما يسهل المرور إلى الفعل الغير مشروع، وهم غالبا يخشون من اكتشافهم وافتضاح أمرهم.

خصائص المُجرم السبيراني:

أثبتت الدراسات بأن المتورطين في الجرائم السيبرانية يتميزون بسمات تميزهم عن غيرهم من المتورطين في الجرائم التقليدية وتالياً أبرز الخصائص المميزة للمجرم السيبراني.

1. مهارة المجرم السيبراني في استخدام التقنية الحديثة لأنظمة المعلومات:

وهي من أهم الخصائص التي تتميز بها المجرم السيبراني والتي تتمثل في إلمام المجرم السيبراني باستخدام الحاسب الآلي والمهارات الفنية بتقنية المعلومات، وقد يكون المجرم السيبراني من المتخصصين في معالجة البيانات الرقمية حيث أن آلية ارتكاب هذه الجريمة تشترط أن يتمتع المجرم بالصفات الفنية الخاصة في استخدام التقنية الذكية .(العتيبي، 2021)

2. المجرم السيبراني على قدر عالي من الذكاء والابتكار:

وهي من أهم خصائص المجرم السيبراني؛لأنه مجرم محترف لديه المعرفة الواسعة في استخد ام الأجهزة الذكية وتسخير التقنية الرقمية لصالحه وتحقيق أهدافه واختراقه الشبكات وكسر كلمات المرور والتعمق في الفضاء السيبراني من خلال القدرة على اخفاء جريمته . (البقمي، 2012)

3. صعوبة الإمساك بالمجرم السيبراني:

تعود صعوبة الإمساك بالمجرم السيبراني إلى ذكائه، لأنه يحرص على إخفاء هويته وتدمير أي دليل يحتمل أن يستدل من خلاله بيئة رقمية الأمر الذي يزيد من صعوبة اكتشاف الجريمة. ويُطلق على المجرم السيبراني بذوي الياقات البيضاء؛ لأنهم ينتمون إلى مناصب رفيعة المستوى .(الديربي، واسماعيل، 2012)

4. خوف المجرم السيبرانيمن كشف الجريمة:

يختص المجرم السيبراني بالخوف من اكتشاف هويته لما يترتب على ذلك من فقدان وظيفتهم ومكانتهم الاجتماعية وسمعتهم، وعليه يتضح بأن المجرم السيبراني

يخشى من اكتشاف جريمته مردها إلى انتمائه في الغالب إلى وسط اجتماعي متميز سواء من حيث التعليم أوالثقافة أوالمستوى المهن.

أصناف المُجرم السيبراني: (الصحفي، 2020)

1. الهواة: وهم من يرتكبون هذه الجرائم بغرض التسلية دون ضرر بالمجني عليه .
2. القراصنة: ومنهم الهاكر: هم متطفلون على أمن النظم المعلوماتية والشبكات من خلال دخولهم إلى أنظمة الحاسبات وكسر الحواجز الأمنية وهدفهم الفضول أوإثبات الذات، ومنهم الكراكر: وهم من يقومون بالتسلل إلى أنظمة المعالجة للاطلاع على المعلومات المخزنة إللحاق الضرر إما بالسرقة أوالعبث بها.
3. المهووسون: ويكون المجرم في حالة الجنون الذي يهدف إلى تحطيم كل الأنظمة.
4. الجريمة المنظمة: فجهاز الحاسب أصبح أداة فعالة بأيدي عصابات المافيا .
5. الحكومات الاجنبية: وذلك باستعمال أجهزة الحاسب في مجال الجاسوسية .
6. المتطرفون: وهم من يستخدمون الشبكة المعلوماتية لنشر أفكارهم السياسية والدينية المتطرفة.

أساليب المُجرم السيبراني لارتكاب الجريمة السيبرانية:

يستخدم المُجرم السيبراني تقنية الإختراق لتنفيذ جريمته وذلك من خلال التحايل على الأنظمة المعلوماتية فيكون الاختراق بالقدرة على وصول هدف مُعين عن طريق ثغرات في نظام الحماية الخاصة، وتتم عن طريق برنامجين الأول الخادم وهوبجاهز الضحية إذ ينفذ المهام الموكلة إليه، والثاني يوجد بجهاز المخترق ويسمى بالبرنامج المستفيد، كما أنهم يستخدمون عدة برامج منها: (خالد، 2020)

1. حصان طراودة: وهوعبارة عن برنامج صغير مختبئ ببرنامج أكبر، وتـؤدي مهامهـا بشكل خفـي في إطلاق الفيروسـات والـدودة التـي تقـوم بإرسـال البيانـات عـن الثغرات الموجودة في النظام، وارسال كلمات المرور السرية الخاصة بالهدف، ومـن أنواعه القنابل المنطقية التي يزرعها المبرمج داخل النظام الذي يطوره.
2. فيروسات الكمبيوتر: وهي برامج صغيرة تستخدم لتعطيل شبكات الخدمات.
3. الديدان: وهـي تكـاثر عـن طريـق نسخ نفسـها عـن طريـق الشـبكات وهـدفها الشبكات المالية مثل البورصات.

صور الجرائم السيبرانية، وهي كالاتي: (الزرقي، 2019)

أولاً: الاعتداء السيبراني عـلى معطيـات الحاسـب الآلي : كـاتلاف البيانـات والمعلومـات والبرامج والتلاعب بالمعلومات المخزنة داخل الحاسب .

ثانيا: الاعتداء السيبراني على حرمة الحياة الخاصة .

أ. يكون بالافشاء العلني للوقائع الخاصة التي تمس الشخص كإفشاء واقعـة إصـابته بمرض مخزي، أوعجز عن سداد ديونه أونشر صورة البنه .

ب. تشويه سمعة الشخص في نظر الجمهور، والتشهير به .

ت. الاستيلاء على بعـض العنـاصر الشخصـية كالاسـم والصـورة والبيانـات الشخصـية المتصلة بالحياة الخاصة.

ثالثا: الاعتداء السيبراني على حقوق الملكية الفكرية : ويكون بالاعتداء عـلى الاعلانـات التجارية وبراءات الاختراع، وكذلك نسخ وتقليد البرامج واعادة إنتاجها وصـنعها دون ترخيص فهواعتداء على الحقوق المالية والحقوق األدبية .

رابعا: الاستيلاء والنصب والاحتيال السيبراني : ويكون الاستيلاء إما لنفسه أولغيره عـلى مال منقول أوعلى سند، أوتوقيع هذا السند، وذلك عن طريق الاحتيال، أواتخاذ اسـم كاذب، أوانتحال صفة غير صحيحة .

خامسا : الانتحال والتغرير السيبراني:

انتحال شخصية فردية: بســبب التنامي المتزايد لشبكة الانترنـت والـذي أعطـى للُمجرمين قدرة أكبر على جمع المعلومات للشــخصية المطلوبـة والاسـتفادة منهـا في ارتــكاب جرائمهــم فتنتشــر في شـبكة الانترنت الكثير مــن الاعلانـات المشــبوهة، والتي تحاكي الطمع الانساني في محاولة الاستيلاء على معلومات اختيارية من الضحية، فهناك اعـلان عـن جـائزة فخمـة يكســبها مــن يســاهم بمبلــغ رمــزي لجهــة خيريــة، وهــذا يتطلب الافصاح عن معلومات ســرية، الأمر الذي يؤدي إلى اسـتيلاء على رصيده البنكي أوالسحب من بطاقته الائتمانية، أوالاساءة إلى سمعة الضحية.

المبحث الثالث: الحماية من الجرائم السيبرانية وطرق التصدي لها وواقع التشريعات الخاصة في مكافحة الجرائم السيبرانية:

الحماية من الجرائم السيبرانية:

يُمكن حماية أجهزة الكبميوتر من الوقوع ضحية للجرائم السيبرانية من خلال اتباع الخطوات الآتية:

أ. تحديث البرامج وأنظمة التشغيل باستمرار.

ت. إستخدام البرامج المضادة للفيروسات وتحديثها باستمرار.

ث. استخدام كلمات مرور قويّة.

ج. عدم النقر على الروابط أوالمرفقات التي تصل مع رسائل البريد الإلكتروني العشوائية.

ح. الحرص على عدم إعطاء أيّة معلومات شخصية ما لم يكن استخدامها آمناً.

خ. التواصل مع الشركات مباشرةً في حال وصول طلبات مشبوهة.

د. المُراقبة المستمرّة لحركات الحساب المصرفي.

آليات المكافحة والتصدي للجرائم السييبرانية:

هنالك العديد من الطرق الموثوقة التي توفر القدرة على مكافحة الجرائم الإلكترونية والتصدي لمنفذيها لحماية أنفسنا ومن حولنا من هذا النوع من الجرائم، والتي تتمثل في نشر التوعية: أي ان نهتم في نشر التوعية الإلكترونية في كل مكان وبين كل الدوائر الاجتماعية التي نعرفه واستحضار القصص كأمثلة لكي يعلم الناس ان كلنا معرضون لمثل هذه المواقف اذا لم نتعلم كيفية استخدام الأجهزة الذكية ومواقع

التواصل الاجتماعي، والاهتمام الفعلي إلى ملُراقبة نشاط الافراد الذين يتعاملون مع الحاسب الآلي والانترنت، في وقت استخدامهم لمواقع التواصل الاجتماعي، ذلك لأن العمر والخبرة والمعرفة هي أسباب رئيسية تُساهم في الحماية من الوقوع في مثل هذه المشاكل والقضايا وتجنب كافة الخسائر بكافة اشكالها وانواعها ، والتي قد تكون كارثية على الافراد والدولة.

وهناك اليات عدة لمُكافحة الجرائم السبيرانية تتمثل بالآتية:

تصدي الهيئات الدولية للجريمة السيبرانية :

مع ارتفاع الخسائر الناتجة عن الاجرام السيبراني وتزايد حجم الاضرار الناتجة عنه، والتي تتخطى في أغلب الاحيان حدود الدول لتصل إعتداءاتها لاجهزة الحواسيب المملوكة للافراد أوالمؤسسات المالية، أوالحكومات ورغم تميز الجرائم السيبرانية بالبعد الدولي كونها جرائم عابرة للحدود الا انها لا تعتبر من الجرائم التي تختص المحكمة الجنائية الدولية بالنظر فيها، والجريمة السيبرانية يُعاقب عليها من خلال التشريعات الوطنية، والسلوك الإجرامي المكون لها يتم على المستوى الداخلي، فهي جرائم داخلية لكن قد يترتب عنها ضرر على المستوى الدولي، لذا إهتمت الهيئات والمنظمات الدولية بمواجهة هذه الجرائم، وعلى رأسها هيئة الامم المتحدة والجمعية الدولية لقانون العقوبات وكذا المجلس الاوربي، ومجلس ووزراء الداخلية والعدل العرب. (مهمل، 2018)

وفي سبيل محاولة التصدي للجرائم السيبرانية تبذل كل من الامم المتحدة، والجمعية الدولية لقانون العقوبات جهوداً لا يستهان بها، تأكيدا على ضرورة تعزيز العمل المُشترك بين جميع الدول. ويشمل هذا التصدي مايلي:

أ. القرار الصادر عن الامم المتحدة بشأن جرائم الكمبيوتر - هافانا 1990 .

بعد إنعقاد مؤتمر الامم المتحدة السابع لمنع الجريمة ومعاملة المجرمين في مدينة ميلانوالايطالية عام1985، والذي تمت من خلاله الاشارة إلى مشكلة الجريمة السيبرانية، حيث إنبثقت عنه مجموعة من التوجيهات من بينها تكليف لجنة الخبراء العشرين لدى منظمة الامم المتحدة، بدراسة موضوع حماية نظم المعلومات والاعتداء على الحاسب الآلي، والتي بدورها أقرت جملة من التوصيات والمقترحات والمبادئ التي تبَناها المؤتمر الثامن لمكافحة الجريمة ومعاملة المجرمين المنعقد 1990 بالعاصمة الكوبية هافانا.(الحسيناوي، 2009)

وتتلخص توصيات مؤتمر هافانا أساسا في التأكيد على ضرورة وضع إطار قانوني دولي بتظافر جهود جميع الدول الاعضاء، من أجل التعاون على الحد من إنتشار وتعاظم آثار هذه الظاهرة الإجرامية المُستحدثة وذلك بأن تقوم كل دولة عضوبتكثيف جهودها لمكافحة إساءة إستخدام الكمبيوتر، وأشار القرار أنه على الدول الاعضاء وفي سبيل مواجهة الاجرام السيبراني إتخاذ مجموعة من الاجرءات تتلخص فيمايلي:(مهمل، 2018)

1-تحديث القوانين وأغراضها الجنائية، من أجل ضمان تطبيق الجزاءات والقوانين الراهنة بشأن وادخال تغييرات مناسبة جهات التحقيق وقبول الادلة في الاجرءات القضائية على نحوملائم، إذا دعت الضرورة إلى ذلك، مع تحسين تدابير أمن الحاسب الاي ومراعاة حماية الخصوصية واحترام حقوق الانسان وحرياته الاساسية، واجرءات تتعلق بالتحقيق والادلة للتصدي لمثل هذا الشكل الجديد والمعقد.

2- وضع أحكام من أشكال النشاط الإجرامي، ومصادرة، أورد الاصول الناجمة عن إرتكاب جرائم ذات صلة بالحاسوب.

3- إعتماد تدابير لزيادة وعي الجماهير والعاملين في الاجهزة القضائية وأجهزة التنايذ، بالمشكلة وبأهمية مكافحة الجرائم ذات الصلة بالحاسب الآلي.

4- إعتماد تدابير مناسبة لتدريب القضاة والمسؤولين عن منع الجريمة الاقتصادية والجرائم المُتعلقة بالحاسب الآلي والتحري والادعاء فيه.

5- الاهتمام بوضع قواعد خاصة بالاداب المتبعة في إستخدام جهاز الحاسب الآلي سياسات تعالج الُمشكلات المتعلقة بضحايا جرائم الحاسب الآلي.

ب. القرارات الصادرة عن المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات بشأن جرائم الكمبيوتر ريودي جانيرو 1994 .

وأوصى المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات الذي إنعقد في ريودي جانيروبالبرازيل في 04 أكتوبر 1994 ، والذي تم من خلاله مناقشة جرائم الحاسب الآلي بأن تتضمن قائمة الحد الادنى من الافعال المشكلة لجرائم الحاسب الآلي والمتعين تجريمها والتي يمكن ذكرها على النحوالتالي: (معتوق، 2012)

- الاحتيال أوالغش المرتبط بالكمبيوتر.
- تزوير الكمبيوتر أوالتزوير المعلوماتي.
- الاضرار بالبيانات والبرامج وتشمل المحووالاتلاف والتعطيل للمعطيات.
- تخريب واتلاف الكمبيوتر.
- الدخول غير المصرح به: وهوالولوج إلى نظام ما عن طريق إنتهاك إجراءات الأمن.
- الاعتراض غير المصرح به: وهوالاعتراض عن طريق وسائل فنية للاتصال توجه لنظام الكمبيوتر أوعدة نظم أوشبكة الاتصالات.

ت. الاتفاقية العربية لمكافحة جرائم تقنية المعلومات .

فقد وافق مجلس وزراء الداخلية والعدل العرب في إجتماعهم المشترك المنعقد بمقر الامانة العامة لجامعة الدول العربية بالقاهرة، على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، تحتوي هذه الاتفاقية على 49 مادة، وجاء في المادة الأولى منها : تهدف هذه الاتفاقية إلى تعزيز التعاون وتدعيمه بين الدول العربية في مجال مُكافحة جرائم تقنية المعلومات لدرء أخطار هذه الجرائم، حاظا على أمن الدول العربية ومصالحها وسلامة مُجتمعاتها وأفرادها، ونجد في الاصل الثاني تأصيل للافعال التي تُعد مُجرمة، أما الاصل الثالث منها فقد تم التعرض من خلاله إلى نطاق تطبيق الاحكام الجزائية، وفي الاصل الرابع نص على التعاون القانوني والقضائي، أما الأصل الخامس فتضمن أحكاما ختامية . (مهمل، 2018)

تصدي التشريعات الغربية والعربية للجريمة السيبرانية:

كان للاتفاقيات الدولية والاقليمة، اثراً بالغاًعلى تشريعات العديد من دول العالم، حيث قامت هذه الاخيرة بتبني فكرة الحماية الجزائية لمُستخدمي شبكة الانترنت ، وكذا البيانات المُخزنة في النظم المعلوماتية، وعليه سيتم التطرق إلى أبرز النماذج التشريعية الغربية والعربية .

أ. تشريعات بعض الدول الغربية.

يُعتبر التشريع البريطاني المكافح للجريمة المعلوماتية من اول التشريعات في مواجهة هذه الجريمة وذلك لريادته في النظام الانجلوسكسوني وكذا التشريع الفرنسي بإعتباره الرائد في النظام اللاتيني.

- **التشريع البريطاني.**

تأتي بريطانيا كثالث دولة قامت بسن قوانين خاصة بجرائم الحاسب الآلي، حيث أقَرت قانون مُكافحة التزوير والتزييف سنة 1981، والذي شمل في تعريفاته الخاصة، تعريف تزوير وسائط التخزين الحاسوبية المتنوعة ، أوأي أداة أخرى يتم التسجيل عليها، سواء بالطرق التقليدية ، أوالإلكترونية أوبأي طريقة أخرى، ثم أصدرت بعد ذلك قانونا خاص بإساءة إستخدام الحاسوب الآلي سنة 1990، الذي نظم جرائم الحاسب الآلي ضمن ثلاث فئات، تتعلق الأولى بالدخول غير المصرح به إلى مُعطيات الحاسب الآلي وبرامجه المخزنة، والثانية فقد تناولت تجريم الدخول غير المصرح به مع وجود نية إرتكاب، أوتسهيل إرتكاب جرائم أخرى، أما الثالثة فتتعلق بتجريم الاتلاف المعلوماتي، وذلك من خلال نص المادة الثالثة من هذا القانون.(الحسيناوي، 2009)

- **التشريع الفرنسي.**

لقد نص المُشرع الفرنسي من خلال قانون العقوبات الفرنسي، على تجريم الاعتداء على أنظمة مُعالجة البيانات، وذلك بموجب الاصل الثالث من الباب الثاني منه، ومن ضمن الجرائم التي نص عليها هذا الاصل، إدخال أومسح أوتغيير معلومات بطرق الغش، المادة 323-3 ما نص أيضا على تجريم عدة أفعال تقع ضد المصالح العليا للدولة، وذلك إذا إنصبت على المعلومات، أوالبيانات التي تمت مُعالجتها إلكترونيا، المواد من 411-6 إلى 411-10 وإلي جانب هذه النصوص، فإن فقد نص المشرع الفرنسي على بعض الجوانب المتصلة بالمُستند الإلكتروني في قوانين متارقة أهمها، قانون الإثبات والتوقيع الإلكتروني الصادر سنة 2001

واللائحة الصادرة سنة 2001 التي أقَر من خلالها الاخذ بالدليل الإلكتروني في الإثبات والتوقيع الإلكتروني.(مهمل ، 2018)

ب. تشريعات بعض الدول العربية.

أصبحت جرائم الإنترنت مشكلة عالمية تؤثر على كل الدول تقريبا، ولا تخضع الجرائم السيبرانية في الوقت الحالي للسيطرة القوية كما يتضح من تفحص المرء للإحصائيات السنوية التي ينتجها معهد أمن الحاسوب (**CSI**) أوالفريق المعني بطوارىء الحاسوب والإستجابة لها (**CERT**)، ووفقاً لمكتب الأمم المتحدة لمكافحة الجرائم والمخدرات (**UNODC**) أن تهديدات سلامة الانترنيت قد إرتفعت بشكل كبير في السنوات الأخيرة، وأن عدد ضحايا الجريمة الإلكترونية على الصعيد العالمي بلغ 431 مليون .

وأمام هذا الرقم من ضحايا التجاوزات الغير مشروعة ومع عدم وجود مواكبة قانونية للمستجدات لهذه الجرائم، أيقنت الدول إلى ضرورة سن القوانين الصارمة للتصدي للجريمة الإلكترونية، وتبني برامج وخطط لمكافحتها، منها إشاعة ثقافة الأمن السيبراني، لذا اصدرت العديد من الدول التشريعات والقوانين الوطنية لمكافحة هذه الجريمة، من أجل ضمان توفير الحماية القانونية الفاعلة للأفراد وللمؤسسات الحكومية والخاصة من هذه الجرائم، وفي بحثنا هذا حرصنا على تناول واقع التشريعات العربية في مكافحة الجريمة المعلوماتية مع إستعراض نموذج من هذه النظم المتمثل في القانون الإتحادي رقم 5 لسنة 2012 لمُكافحة الجرائم الإلكترونية لدولة الإمارات العربية المتحدة. (الكيلاني ، 2013)

واقع التشريعات والممارسات لمكافحة الجرائم الإلكترونية:

مع إتساع إستخدام الفضاء الإلكتروني كشبكات التواصل الاجتماعي أصبحت الجريمة الإلكترونية أكثر تنوعاً. وتلعب أجهزة الكمبيوتر والإنترنت دورا أساسيا في تسهيل ارتكاب الجرائم التقليدية بطرق عدة، فمواقع الفيسبوك وتويتر وغيرها من مواقع الشبكات الاجتماعية يمكن أيضا أن تستخدم من قبل المجرمين ، وأكدت دراسة شركة الخليج للحاسبات الآلية **G.BM** في يونيو2013 أن خبراء تكنولوجيا المعلومات في دول مجلس التعاون يؤكدون أن منطقة الخليج تشكل هدفاً رئيسياً للجرائم الإلكترونية كما ذكرت الدراسة أن زيادة شبكات التواصل الإجتماعي يصاحبه إزدياد في مخاطر الأمن الإلكتروني.(سكولمان، 2007)

وورد في تقرير نورتن سيمانتيك" **Norton Symantec** " لعام 2013 أن كلا من المملكة العربية السعودية، ودولة الامارات العربية المتحدة من دول مجلس التعاون الخليجي، ضمن الـ 24 دولة الأولى في العالم التي تزيد فيها التهديدات المقلقة بتسرب البيانات، حتى وقتٍ قريب، كان للحكومات مقاربات مختلفة بشأن التشريعات الخاصة بالإنترنت. فمعظم دول العالم تنظّم الإنترنت ضمن حدود قيمها السياسية والقانونية والأخلاقية والثقافية، لكن بما أن تطوّر تكنولوجيا الإتصالات والمعلومات يجري على مستوى دولي خارجًا عن نطاق سيطرة هذه الدول، فإن اعتماد تشريعات فعالة وتنفيذها لمكافحة جرائم الإنترنت يشكّل تحديًا كبيراً للحكومات. وبالتالي إن جرائم الإنترنت تمثّل تحديًا كبيراً للأجهزة القانونية في كلّ من البلدان المتقدمة والنامية . (الجنابي، 2017)

وبينت دراسات الإسكوا الفجوة القانونية، في مجال التشريعات السيبرانية، بين البلدان العربية والبلدان المتقدمة من جهة، وبين البلدان العربية نفسها من جهة

أخرى. ونظراً للطبيعة الشمولية للفضاء السيبراني وتجاوزه حدود البلدان والأقاليم، فالتنسيق الدولي والإقليمي مهم جداً بالنسبة للتشريعات السيبرانية، ويأخذ البعد الإقليمي أهمية كبرى بالنسبة للمنطقة العربية إذ يساهم تنسيق التشريعات السيبرانية في المنطقة العربية ببناء مُجتمع معرفة عربي متكامل من خلال التعاون والتنسيق لمواجهة المخاطر المعلوماتية، وتحفيز المعاملات والخدمات الإلكترونية بين البلدان العربية، والمساهمة في حماية الملكية الفكرية للفضاء السيبراني على المستوى الإقليمي العربي .

وضمن جهود مجلس وزراء العدل العرب في مكافحة الجرائم السيبرانية قرر إعتماد " قانون الإمارات العربي الإسترشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها (2004) " يتكون القانون من (27) مادة التي عالجت موضوع الجرائم الإلكترونية، وعن مبادرة تحديث وتطوير عمل النيابات العامة في الدول العربية التي يقوم بتنفيذها برنامج الأمم المتحدة الإنمائي - برنامج إدارة الحكم في الدول العربية **UNDP -POGAR** منذ العام 2002 م، تم تنظيم مجموعة من الانشطة تتضمن ندوات تثقيفية ودورات تدريبية بغية توطيد المعرفة لدى أعضاء النيابات العامة حول الجرائم الحديثة من أجل تفعيل دورهم في تعزيز حكم القانون وبناء قدراتهم لجهة إستخدام أساليب ومنهجيات التحقيق المتطورة. وقد ركز المشروع ضمن إطار نشاطاته على موضوع مكافحة الجرائم الإلكترونية، وتحقيقا لهذه الغاية قام بتنظيم ندوة إقليمية تحت عنوان " الجرائم المتصلة بالكمبيوتر"، وذلك في المملكة المغربية بتاريخ 20/19 يونيو2007، وذلك بناء على طلب من النيابات العامة في عدد من الدول العربية، ولقد هدفت هذه الندوة إلى تعزيز وبناء

معرفة النيابات العامة بالجرائم المتعلقة بالكمبيوتر والاساليب والتقنيات الحديثة المُستخدمة لمواجهة هذا النوع من الجرائم .(الجنابي، 2017)

وقامت الدول العربية بوضع العديد من القوانين السيبرانية في السنوات الخمس الأخيرة، وتعتبر قوانين التعاملات الإلكترونية بما فيها التوقيع الإلكتروني من أكثر القوانين انتشاراً في المنطقة العربية، وقامت العديد من الدول بوضع قوانين للجرائم السيبرانية، وتعاني معظم الدول من نقص في مجال التشريعات الخاصة بمحاور مُعالجة وحماية البيانات ذات الطابع الشخصي، وحماية المُستهلك في التعاقدات الإلكترونية، والمسائل المتعلقة بالملكية الفكرية على الإنترنت.

وقامت بعض الدول العربية بسن تشريعات تقوم بمكافحة الجريمة السبيرانية حيث تعد دولة الامارات العربية المتحدة من الدول العربية القليلة والرائدة في مجال التشريع الخاص بحماية النظم المعلوماتية وقد تناول القانون الاتحادي رقم 02 لسنة 2006 المُتعلق بمكافحة جرائم المعلوماتية، مجموعة من الجرائم، كجريمة إختراق المواقع والأنظمة الإلكترونية، أين تم التمييز بين الأنظمة المعلوماتية وبين الاختراق، وترتب نتيجة مُتعلقة بالالغاء أوالحذف ، أوتدمير المعلومات، إذ جعل العقوبة في الحالة الثانية أشد وتقدر بالحبس لمدةّ ل تقل عن 6 أشهر مع غرامة مالية، وفي حالة إختراق النظم المعلوماتية يترتب عن ذلك إنتهاك للمعلومات الشخصية، وتكون العقوبة هي الحبس لمدة لا تقل عن سنة، وغرامة مالية مقدرة بعشرة ألّف درهم.(معتوق، 2012)

- **التشريع المصري**

لقد وضع المؤتمر التأسيسي الأول لجمعيات قانون الانترنت الذي عقد بالقاهرة في 27 سبتمبر 2004 اللبنة الأولى لانشاء جمعيات ومنظمات للعمل التطوعي في مجال قانون الانترنت، ثم تم عقد المؤتمر الدولي الأول لقانون الانترنت بمدينة الغردقة في العام 2005 وبدأ الاهتمام في مصر بمُكافحة الجرائم المعلوماتية.

ثم تأسست الجمعية المصرية لمكافحة جرائم المعلوماتية في نفس السنة، وهي منظمة غير حكومية تعمل على نشر الوعي واعداد الدراسات والمؤتمرات حول هذه الجرائم، وتعتبر حركة التشريع في مجال مُكافحة الجريمة السيبرانية في مصر، ضعيفة مُقارنة بدولة الامارات العربية المُتحدة، الا ان تطبيق بعض النصوص التقليدية المُتعلقة بالتزوير والاحتيال والسرقة، والمساس بإعتبار الاشخاص، لا يزال مُستمراً في القانون المصر.(معتوق، 2012)

ويُعتبر قانون التوقيع الإلكتروني الصادر سنة 2004، أول قانون يصدر بشأن الافعال المتعلقة بالنظم المعلوماتية في مصر، حيث جرم أفعالّ بموجب المادة 23 منه، تتعلق بالحصول على توقيع أووسيط أومحرر إلكتروني بدون وجه حق، أوإعتراضه، أوتعطيله عن أداء وظيفته وقد عرف الوسيط الإلكتروني في الفقرة الرابعة من المادة الأولى من قانون التوقيع الإلكتروني المصري بأنه أداة أوأدوات، أوأنظمة إنشاء التوقيع الإلكتروني، فهوعبارة عن نظام معلوماتي يُساعد على إنشاء التوقيع الإلكتروني، واصدار المحررات الإلكترونية . (مهمل، 2018)

وفي الأردن صدر قانون المُعاملات الإلكترونية لسنة 2015، والذي تضمن مواد عدة تتمثل في يكون أي كلمات اوعبارات، حيثما وردت في هذا القانون والمعاني المخصصة لها ما لم تدل القرينة على غير ذلك، وان ما يتعلق بالمعاملات

وأي إجراء يقع بين طرف أوأكثر ينشئ التـزام عـلى طـرف واحـد أوالتـزام تبـادلي بـين طرفين أوأكثر سواء كان يتعلق هذا الاجراء بعمل تجـاري أومـدني أويكـون مـع دائـرة حكومية، وان المعـاملات الإلكترونيـة هـي التـي تنفـذ بوسـائل إلكترونيـة، وان كافـة الوسائل الإلكترونية هـي تقنيـة إسـتخدام وسـائل كهربائيـة أومغناطيسـية أوضـوئية أوكهرومغناطيسية، أوأي وسـيلة مشـابهة، وان كافـة المعلومـات الإلكترونيـة تتضـمن البيانات أوالنصوص أوالصور، أوالرسـومات أوالاشـكال أوالاصـوات، أوالرمـوز أوقواعـد البيانات وما شابه ذلك.

مراجع الفصل الثالث

المراجع العربية.

1. البداينة ، ذياب موسى ، (2014)، " الجرائم الإلكترونية المفهوم والاسباب "، ورقة علمية مقدمة في الملتقى العلمي الجرائم المُستحدثة في ظل المتغيرات والتحولات الاقليمة والدولية، خلال الفترة من 20-20 سبتمبر كلية العلوم الاستراتيجية، عمان- الأردن.
2. البقمي محمد ، (2012)، أهمية الأدلة الرقمية في الإثبات الجنائي: دراسة وفق الأنظمة السعودية، مجلة الفكر الشرطي، المجلد(21)، العدد(80).
3. بلعزوق، عبدالمكريم، (2017)، دراسة في ماهية الاجرام الإلكتروني ومجرم الانترنت"، مداخلة مقدمة ضمن فعاليات الملتقى الدولي الذي نظمته كلية الحقوق والعلوم السياسية قسم الحقوق جامعة برج بوعريريج، الموسوم بعنوان: الإجرام السيبراني المفاهيم والتحديات، 11-12 نيسان .
4. بن داود، عبدالعزيز بن فهد، (2020)، الجرائم السيبرانية: دراسة تأصيلية مقارنة، مجلة الأجتهاد للدراسات القانونية والإقتصادية مجلد (9) ، العدد 3، لسنة 2020.
5. جعفر، علي ، (2013)، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الاشخاص والحكومة، الطبعة منشورات زين الحقوقية، الطبعة الأولى بيروت- لبنان .
6. الجنابي، ليلي، (2017)، فعالية القوانين الوطنية والدولية في مكافحة الجرائم السيبرانية، مجلة الحوار المتمدن ، العدد5643.

7. الحسيناوي، علي جبار ، (2009)، جرائم الحاسوب والانترنت، دار اليازوري العلمية للنشر والتوزيع، عمان-الأردن .

8. دريس، نبيل، (2013)، الجريمة السيبرانية بين المفاهيم والنصوص التشريعية "الجزائر أنموذجا"، مجلة القانون والمُجتمع، العدد (11)، الجزائر.

9. الديربي عبدالعال، واسماعيل ، محمد صادق ، (2012) ، الجرائم الإلكترونية، دراسة قانونية قضائية مقارنه مع أحدث التشريعات العربية في مجال مكافحة جرائم المعلوماتية والإنترنت، المركز القومي للإصدارات القانونية، القاهرة- مصر.

10. الزرفي ، علي نعمة جواد (2019)، الجريمة المعلوماتية الماسة بالحياة الخاصة دراسة مقارنة، المكتب الجامعي الحديث ، الاسكندرية – مصر .

11. سحواذ، نسيمة ، (2015)، الجريمة الإلكترونية مشكلة عالمية، مجلة الشرطة للمديرية العامة للامن الوطني، العدد 129، ديسمبر، الجزائر .

12. سكولمان، كرستينا، (2007)، برنامج تعزيز حكم القانون في بعض الدول العربية، اعمال الندوة الاقليمية حول الجرائم المتصلة بالكمبيوتر، الرباط- لمملكة المغربية.

13. الشمري، غانم مرضي ، (2016)، الجرائم المعلوماتية، الدار العلمية الدولية، الطبعة الأولى، عمان – الأردن .

14. الصحفي، روان بنت عطية الله ، (2020)، الجرائم السبيرانية، المجلة الإلكترونية الشاملة متعددة التخصصات، العدد الرابع والعشرين، شهر5.

15. العتيبي، زياد بن محمد ، (2021)، جرائم السيبرانية المرتكبة عبر الوسائط الرقمية وبيان مفهومها من حيث: أشكالها، خصائصها، أركانها والدافع من

ارتكابها المجلة العالمية للدراسات القانونية ، المجلة الاكاديمية العالمية للدراسات القانونية، العدد1، المجلد 3.

16. القحطاني، مداوي سعيد، (2016)، الجريمة الإلكترونية في المُجتمع الخليجي وكيفية مواجهتها، مجلس التعاون الخليجي ، مسابقة جائزة الامير نايف بن عبدالعزيز للبحوث الأمنية لعام (2015م(، الرياض- السعودية.
17. الكيلاني ، عبد الله حامد ، (2013)، جهود مكافحة الإرهاب النووي على الصعيد العربي، قطاع الشؤون القانونية جامعة الدول العربية، الرياض- السعودية.
18. معتوق، عبداللطيف ، (2012) ، الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن، رسالة ماجستير غير منشورة، جامعة العقيد الحاج لخضر بباتنة، كلية الحقوق والعلوم السياسية الجزائر.
19. مقال منشور، الوطن/ ارم نيوز، البحرين، 2022)
20. مهمل، اسامه ، (2018)، الاجرام السيبراني، رسالة ماجستير غير منشورة، كلية الحقوق والعلوم السياسية جامعة محمد بوضياف، الجزائر.

المراجع الاجنبية.

- **The Transnational Dimension (Goodman, 2000 &Seymour, Abraham Sofaer), Cyber Crime and Security, DP5 HPCYBE0100 06-25-:1 11:43:01 rev1.**

-Tripathi ،Shambhavi, (2019), Cyber Crime and Cyber Security: An overview, https://blog.ipleaders.in/cyber-crime-and-cyber-security -an-overview.

- **Tips on how to protect yourself against cybercrime, (2021), www.kaspersky.com.**

الفصل الرابع

الجريمة الإلكترونية

(منظور قانوني)

الفصل الرابع

الجريمة الإلكترونية

(منظور قانوني)

المقدمة:

إن المشروع الأردني حظر على الموظف العام إفشاء أسرار الوظيفة العامة حتى أمام القضاء إلا في أحوال محددة، وبناء على نصوص قانونيه خاصة أوبموافقة الجهة الإدارية التي يعمل لديها فعلى سبيل المثال، لم يجز قانون البيانات رقم(30) لسنة 1952 للموظفين المستخدمين والمكلفين بخدمة عامة، أن يشهدوا ولوبعد تركهم العمل بما يكون قد وصل إلى علمهم أثناء قيامهم بالعمل من معلومات لا يجوز إفشائها إلا بقرار من المحكمة، كما لم يجز أن يشهد احد ولولم يكن موظفا عاما، على معلومات أومضمون أوراق تتعلق بشؤون الدولة، إلا إذا كانت قد نشرت بالطريق القانوني، أوكانت السلطة المختصة قد أذنت في إذاعتها.(قانون البيانات، 1952)

إن الحاسوب قد يكون هدفا لنشر الوثائق المحمية دون علم الجهات الإدارية والمدنية بذلك كما في حالة الدخول غير المصرح به إلى النظام، أوزراعة الفيروسات لتدمير المعطيات والملفات المخزنة أوتعديلها، وكما في حالة الاستيلاء على البيانات المخزنة أوالمنقولة عبر النظم، وقد يكون الحاسوب أداة لنشر الوثائق الرسمية المحمية كما في حالة استغلال الحاسوب للاستيلاء على الأموال بإجراء تحويلات غير مشروعة، أواستخدام التقنية في عمليات التزييف والتزوير، أواستخدام التقنية في الاستيلاء على أرقام بطاقات ائتمان وإعادة استخدامها والاستيلاء على

الأموال بوساطة ذلك، وقد يكون الحاسوب بيئة الجريمة، وذلك كما في تخزين البرامج المقرصنة فيه أوفي حالة استخدامه لنشر المواد غير القانونية أواستخدامه أداة تخزين أواتصال لصفقات ترويج المخدرات وأنشطة الشبكات الإباحية ونحوها.(يونس، 2002)

وفي مجال المسؤولية الناشئة عن إساءة استخدام الحاسوب والإنترنت، لا تثور أية مشكلة فيما يتعلق بالجرائم الإلكترونية فإذا تم إدانة الشخص بأية جريمة جزائية- أيا كانت درجتها - ارتكبت بوساطة أجهزة الحاسوب والإنترنت، أوعلى مكونات الحاسوب المادية منها وغير المادية، فإن هذا الحكم وحده يكفي للمطالبة بالتعويض عن الفعل الضار المرتكب، فالجريمة سواء أكانت إلكترونية أم غيرها تشكل دائما وابدا فعلا ضارا يوجب التعويض عن الضرر الناجم عنها.

ورغم انفصال وتباين نطاق وأساس المسؤولية الجزائية عن نطاق وأساس المسؤولية المدنية إلا أن التشريعات درجت على منح الحكم الجزائي حجية أمام المحاكم المدنية، ويجوز للقاضي المدني وقف الدعوى المدنية إلى أن يتم الفصل في الدعوى الجزائية، فإذا تم الفصل في وقوع الفعل ووصفه القانوني ونسبته إلى فاعله فإنه يشترط لحجية الحكم الجزائي: (قانون أصول المحاكمات، 1988)

- أن يفصل الحكم الجزائي في الوقائع المعروضة على القاضي المدني.
- أن يكون فصله في الوقائع ضروريا.

وهذا يعني أن القاضي المدني يتقيد بالوقائع التي حصل فيها القاضي الجزائي دون أن يتقيد بالتكيف القانوني الذي تضمنه الحكم الجزائي لهذه الوقائع من الناحية الجزائية.(القضاة، 1998)

فالحكم الجزائي الصادر بالإدانة يلزم القاضي المدني ولا يكون أمامه سوى البحث في تقدير التعويض عن الضرر الناجم عن هذه الجريمة، أما الحكم الجنائي الصادر بالبراءة فإما أن يصدر بالبراءة لعدم نسبة الفعل إلى المتهم وفي هذه الحالة يمتنع على القاضي المدني الحكم بالتعويض لأن الحكم بالتعويض معناه وقوع الفعل من المتهم فيتناقض الحكم المدني مع الحكم الجزائي، أما إذا صدر بالبراءة لأن الفعل الواقع من المتهم، لا يعد جريمة جنائية أولأن الدعوى الجزائية لم تعد مسموعة، وإما لوجود مانع من موانع العقاب، فيجوز للقاضي المدني مع ذلك الحكم بالتعويض، لأنه لا تعارض في هذه الحالات بين الحكم بالتعويض في الدعوى المدنية وبين الحكم بالبراءة في الدعوى الجزائية. (سلطان، 2011)

وفي هذه الجزئية تقول محكمة التمييز الأردنية "إن المادة 332 من قانون أصول المحاكمات الجزائية تنص على أن الحكم الجزائي يحوز قوة الشيء المحكوم به أمام المحاكم المدنية فيما يتعلق بموضوع الجريمة ووصفها القانوني ونسبتها إلى فاعلها، وعليه فإن محكمة البداية مقيدة بما جاء في الحكم الجزائي من حيث تحديد فاعل الجريمة ولا مجال لإثبات عكس ذلك".(قرار محكمة التمييز الأردنية، رقم 74/45، 1974)

المبحث الأول: الجريمة الإلكترونية (جريمة نشر وتسريب الوثائق المحمية عبر وسائل التواصل الاجتماعي)

إن ثبوت المسؤولية الجنائية الإلكترونية في تسريب المعلومات والوثـائق المحميـة يؤثر بالضرورة في المسؤولية المدنية عن ذات الفعـل، فهـي تتمثـل في تعـويض الجهـة المتضررة عما حل به من أضرار مادية وأدبية بسـبب التسريـب الإلكـتروني، والـدعوى المدنية التي يرفعها المتضرر هي وسيلة الحصول عـلى التعـويض، ونظـرا لأن الجريمـة الإلكترونية تقوم بصفة أساسية على حمايـة التجـارة الإلكترونيـة، فإنـه يترتـب عليهـا بالضرورة في كل الأحوال تقريبا، وقوع ضرر مادي أوأدبي لجهة ما سواء أكانت فرديـة أم جماعية أم مؤسسة ما، ومن ثم ميلاد المسؤولية المدنية التي يسهل إثباتها والفصل فيها في هذه الحالة.(منصور، 2012)

أركان الجريمة الإلكترونية

في القانون الأمريكي(رمضان، 2004). وفي عـام 1984 (المنشـاوي، 2005) صـدر في الولايات المتحدة الأمريكية القانون الفيدرالي في شأن الاعتداء عـلى مؤسسـات الدولـة والأفراد من خلال الحاسوب واستغلاله وعـدل في أعـوام 1986 و 1994 و 1996 وورد في الفصل 1030 من نصـوص خاصـة تجـرم الاعتـداء مـن خـلال الحاسـوب والأعـمال المتعلقة بأنشطة متصلة به. وكذلك ورد في قانون الجرائم الإلكترونية المادة (44) مـا نصه:" مع عدم الإخلال بأية عقوبة اشد ورد في قانون آخـر يعاقـب بـالحبس لمـده لا تزيد عن ثلاثة سنوات وبغرامه لا تزيد عن 6000 دينار أوما يعادلها بالعملة المتداولة قانونا أوبإحدى هاتين العقوبتين كل من: (رمضان، 2004)

كشف مفاتيح لفك التشفير أوفك تشفير معلومات بـأي طريقـة في غـير الأحـوال المصرح بها قانونا. والمادة (3) من قانون الجـرائم الإلكترونيـة رقـم (27) لسـنة 2015 تنص على: " يعاقب كل من دخل قصداً إلى الشبكة المعلوماتية أونظام معلومات بأي وسيلة دون تصريح أوبما يخالف أويجاوز التصريح، بالحبس مدة لا تقل عـن أسـبوع ولا تزيد على ثلاثة أشهر أوبغرامة لا تقل عن (100) مائة دينار ولا تزيد عـلى (200) مائتي دينار أوبكلتا هاتين العقوبتين".

- استعمل بصفه غير مشروعة أداة إنشاء توقيع أوعناصر تشـفير شخصـيه متعلقـة بتوقيع شخص آخر.
- إنشاء أونشر شهادة أوالزور معلومات الكترونية غير صحيحة لغرض غير مشروع.
- حصل بطريق الغش على معلومات محمية من نظام حاسب إلى خاص بالغير.
- أفشى معلومات خاصة بالغير حصل عليها أثناء تسجيلها أوإرسالها بأي وسيله من وسـائل المعالجـة المعلوماتيـة وكـان مـن شـان إفشـائها المسـاس بـس معـه وخصوصيات صاحبها أوالغير.
- منع عمدا أحد رجال الضبطية القضائية أوالمخول لهم قانونا بإجراء تفتيش لنظام الكتروني.

ويعاقب الفصل1030 أي شـخص يـدخل عمـدا إلى جهـاز حاسـوب دون تصريـح أويحصل متجاوزا التصريح الممنـوح لـه بـأي وسـيلة كانـت عـلى معلومـات حـددت حكومة الولايات المتحدة الأمريكية أنه لا يجوز الكشف عنهـا لأمـور تتعلـق بالـدفاع الـوطني أوالعلاقـات الخارجيـة، أوأي بيانـات ووثـائق سريـة كتلـك المتعلقـة بـالأمور المحددة بالفقرة (ي) من الفصل الثاني من قـانون الطاقـة النوويـة الصـادر في 1954،

وذلك إذا اتجهت إرادة الجاني أوتوافر الاعتقاد أن مثـل هـذه المعلومـات ستسـتخدم للمساس بالولايات المتحدة الأمريكية أوبمصالح أي دولة أجنبية(رمضان، 2004).

كما يعاقب القانون كل من يقوم عمدا بالدخول على جهاز حاسوب دون تصريح أوتجاوز التصريح الممنوح له ويحصل على معلومات مجمدة في سجل اقتصادي يخص مؤسسة مالية أويخص مانح بطاقات ماليـة أوالمعلومـات الموجـودة في تقريـر يتعلـق بالمستهلكين، ويعاقب القانون كذلك على الـدخول العمـدي عـلى البيانـات الموجـودة بأجهزة الحاسوب الخاصة بالوكالات والجهات، والتي يقتصر اسـتعمالها عـلى حكومـة الولايات المتحدة الأمريكية، وإذا كان الاستعمال لا يقتصر كلية على حكومة الولايـات المتحدة الأمريكية ولكنه يستعمل لمصلحتها وكان من شأن الدخول على الحاسوب أن يؤثر في مثل هذا الاستعمال.

ويعاقب المشرع الأمريكي كذلك كل من يدخل عـلى جهـاز حاسـوب يسـتخدم في التجارة أوالاتصال بين الولايات ويقوم عمدا بنقل **Transmission** لبرنامج أومعلومة أوكود حاسوب أونظام للحاسوب، ويعاقب أيضا كـل مـن يمنـع أويحـرم أويتسـبب في منـع أوحرمـان الغـير مـن اسـتعمال حاسـوب أوخـدمات حاسـوب أونظـام أوشـبكة أومعلومـات أوبيانـات أوبرنـامج، وكـذلك يعاقـب عـلى نقـل أي مكونـات لـبرامج أومعلومات أوكود أوأمر دون موافقة من المسؤولين على الحاسوب المستقبل للبرنـامج أوالمعلومات أوالكود أوالأمر إذا أدى هذا النقل إلى خسـائر لشـخص أوأكثرتبلـغ ألـف دولار أوأكثر خلال فترة سنة من ارتكاب الفعـل أوإذا أدت إلى تعـديل أوإفسـاد كـلي أوجزئي لكشف طبي أوتقرير طبي أوعلاج طبـي أوالرعايـة الصـحية لشـخص أوأكـثر. (رمضان، 2004)

ويعاقب كذلك على القيام بنقل برنامج أومعلومات أوكود أوأمر بطريق الحاسوب لجهاز يستخدم في التجارة أوالاتصال بين الولايات، إذا أضر النقل أوتسبب في الأضرار لحاسوب أولنظام الحاسوب أولشبكة أوالمعلومة أوبيان أولبرنامج وكان ذلك دون تصريح من المسؤولين عن النظام الذي نقل إليه البرنامج أوالمعلومة أوالكود أوالأمر وتسبب في خسائر تقدر بألف دولار أوأكثر خلال فترة سنة أوعدل أوعطل كليا أوجزئي التقارير الطبية، ويعاقب أيضا على غش كلمات المرور بما يسمح بالدخول على نظام للحاسوب دون تصريح إذا كان من شأن ذلك الإضرار بالتجارة بين الولايات أوبالتجارة الخارجية، كما أن القانون الأمريكي قرر عقوبات مشددة للجرائم المشار إليها والشروع فيها. (المنشاوي، 2005)

ومع كل ذلك فقد كشف التقرير الصادر عن لجنة عمل رئيس الولايات المتحدة الأمريكية السابق الإشارة إليها، أن القانون ينطوي على الكثير من الغموض والقصور بحيث يمكن للمجرمين تلافي تطبيق القانون عليهم باستخدام حاسبات وشبكات تقع خارج الولايات المتحدة الأمريكية، كما يمكن لمجرمي الحاسوب من خارج الولايات المتحدة الأمريكية استخدام الأنظمة الموجودة بالدولة للاعتداء على وثائق محمية في حاسبات تقع في دول أخرى.(**Usdoj,2017**)

وفي المجلس الأوروبي شعر المجتمع الأوروبي بخطورة جرائم الحاسوب، ولذلك عملت اللجنة الأوروبية بشأن مشاكل الجريمة ولجنة الخبراء في مجال الحاسوب على إعداد مشروع اتفاقية تتعلق بجرائم الحاسوب (**DRAFT NO19**)، وقد أعلن المجلس الأوروبي مشروع هذه الاتفاقية في 2000/4/27(المنشاوي، 2005)، ولقد أكد المجلس الأوروبي أن الاعتداءات الحديثة على مواقع الوثائق المحمية من خلال الإنترنت من خلال استخدام موقع أمازون دوت

كـوم**amazon.com** هـي التـي وجهـت نظـر المجتمـع الـدولي إلى المخـاطر التـي تواجهها الوثـائق عـبر الإنترنـت وشـبكات الحاسـوب، وأن جـرائم الحاسـوب تهـدد الوثائق المحمية والمصالح الحكومية، ولذلك فلقد أخذ المجلس زمام المبادرة ووضع مشروعا لاتفاقية تتعلق بجرائم الحاسوب مع الأخذ بعـين الاعتبـار الطـابع الـدولي الغالـب المثـل هـذه الجـرائم(**cybercrime,2021**)، وقـد وضـع مشروع الاتفاقيـة تعريفات فنية لبعض المصطلحات الخاصة بالحاسب واسـتعمالاته، ويـنص المشروع على الإجراءات التي يتعين اتخاذها بالدول المتعاقدة على المسـتوى الـداخلي وعـلى المستوى الدولي، فعـلى المسـتوى الـداخلي يوجـه المشروع الـدول المتعاقـدة إلى أن تجرم أفعال الاعتداء على سرية وتكامل الوثـائق والبيانـات في الحاسـوب وأنظمتـه والاتصال بها، وحدد المشروع من هذه الأفعال الدخول العمدي غـير المشروع عـلى نظام الحاسوب بصورة كلية أوجزئيـة، ويمكـن للـدول المتعاقـدة أن تضـيف شرطـة للعقاب وهوأن يكون الدخول باختراق إجراءات تأمين النظام أوبنية الحصـول عـلى بيانات معينة أولأي غرض آخر غير مشروع. ومن الأفعال التـي عـدها المشروع مـن الجرائم الالتقاط العمدي بأي وسيلة تقنية لأي نقل لبيانات حاسوب مـن أوداخـل نظام للحاسوب، وكذلك يعد جريمة أي إرسال كهرومغناطيسي من نظام للحاسـوب يحمل مثل هذه المعلومات وكذلك الإتلاف أوالحذف أوالتعديل أوالمسـح العمـدي لأي من بيانات الحاسوب دون حق وكـذلك عـد جريمـة الإعاقـة العمـد دون حـق لعمل نظام للحاسوب بإدخال أونقل أوإتلاف أوتعديل أوإلغـاء بيانـات الحاسـوب، وعد المشروع من الجرائم كذلك إنتاج أوبيع أوحيازة أواستيراد أوتوزيع أوتـوفير أي 1- وسيلة بما فيها برامج الحاسـوب المصـممة أوالمعـدة خصيصـا لارتكـاب الجـرائم المشار إليها، 2- وكذلك كلمة سر أوكود للدخول أوأي بيـان مشـابه يمكـن الـدخول

عن طريق أي منها على نظام الحاسوب لارتكاب الجرائم المشار إليها. (المجلس الأوروبي، 2004)

ومن الجرائم الملحقة بجرائم الحاسوب تزييف الوثائق من خلال برامج الحاسوب، وتتحقق هذه الجريمة بالإدخال أوالتعديل أوالتبديل أوالمسح العمدي لبيانات متعلقة ببيانات مزيفة بنية استخدامها من الناحية القانونية كما لوكانت أصلية، ولا يشترط أن يكون في الإمكان قراءة هذه البيانات أوأن تكون واضحة، وقد يشترط طرف من أطراف الاتفاقية توافر نية الغش أوأي نية أخرى غير مشروعة لإقامة المسؤولية الجنائية، ويعد جريمة ملحقة بجرائم الحاسوب أي التسبب العمدي في فقد ملكية أي شخص أ بإدخال أوتعديل أوإلغاء أومسح بيانات تخص الحاسوب، ب - بالتدخل في عمل الحاسوب (البرنامج) أوالنظام بقصد الحصول دون حق على فائدة اقتصادية لنفسه أوللغير، وتناولت المادة العاشرة من المشروع جريمة الاعتداء على وثائق الملكية الفكرية والجرائم الملحقة بها، واتفقت الدول المتعاقدة على أن تجرم في قوانينها الداخلية التقليد والتوزيع بطريق أنظمة الحاسوب للأعمال المحمية بقوانين الملكية الفكرية وفق القانون الوطني (استنادا لاتفاقية برن لحماية الأعمال الأدبية والفنية واتفاقية التريس ومعاهدة الوايبوللملكية الفكرية، وذلك إذا ارتكبت هذه الأفعال وبصورة الاتجار عمدا ودون حق، وأجاز المشروع لأي طرف من الأطراف تجريم تقليد وتوزيع بوساطة نظام للحاسوب أعمال أواختراعات محمية وفق قانون الدولة واستنادا لمعاهدة بيرن بشأن الأداء والفونوجرام.

وتناولت المواد 11 و12 و13 الأحكام الخاصة بالمساهمة التبعية والشروع ومسؤولية الأشخاص المعنوية والعقوبات، وتناول المشروع كذلك تنظيما للإجراءات الجنائية والتعاون الدولي في مجال جرائم الحاسوب.

تناول المشرع الفرنسي في الكتاب الثالث من قانون العقوبات الجديـد، الجنايـات والجنح التي تقع على الأموال، وخصص الباب الثاني منه للجرائم الأخرى على الأمـوال وخصص الفصل الثالث من هذا الباب لجرائم الاعتداء على أنظمة معالجـة البيانـات، فتناول مجموعة من الجرائم التي تقع على أنظمة معالجة البيانات 323 - 1 إلى 323 - 7، وتعاقب المادة الأولى على الدخول بطريق الغش أوالتدليس على أوإبقاء الاتصال بطريقة غير مشروعة نظاما لمعالجة البيانات بالحبس لمدة سـنة وبغرامـة مائـة ألـف فرنك فرنسي، وضاعف العقوبة إذا ترتب على نشاط الجاني إلغـاء أوتعـديل البيانـات الموجودة بالنظام أوتعديل تشغيل النظـام (م323 - 2). (قـانون العقوبـات الفـرنسي، 2020)

كما تعاقب المادة الثانية على إعاقة أوالتسبب في تحريف تشـغيل نظـام معالجـة البيانات، في حين تعاقب المادة الثالثة على عملية إدخال بيانات بطريقة غير مشروعة في نظـام معالجـة البيانـات أوإلغـاء أوتعـديل البيانـات التـي يحتويهـا بطريقـة غـير مشروعـة (م323 – 3)، تعاقـب المـادة 323 - 4 المسـاهمة في جماعـة أوالاتفـاق بـين مجموعة من الأشخاص للتحضير بعمـل أوأعـمال ماديـة لارتكـاب جريمـة أوأكـثر مـن الجرائم السابقة، وتقرر المادة 323 5 بعض العقوبات التكميلية منها: مصـادرة الشيء أوالأشياء التي استخدمت في ارتكـاب الجريمـة، الإغـلاق لمـدة لا تزيـد عـن 5 سـنوات للأماكن أوالمشروعات التي استخدمت في ارتكاب الجريمـة، إعـلان ونشر الحكـم، كـما أجاز المشرع الفرنسي مساءلة الأشخاص المعنوية بذات الأحكام العامة لمسألتهم، كـما قـرر المشرع معاقبـة الشروع في ارتكـاب الجـرائم السـابقة بـذات العقوبـات المقـررة للجريمة التامة. (المنشاوي، 2005)

أي أن المشرع الفرنسي أقام بهذه النصوص ثلاث أنواع من الجرائم وهي: الدخول العمدي غير المشروع على نظام لمعالجة البيانات، وإعاقة تشغيل النظام، وإدخال أوإلغاء بيانات في برنامج معالجة البيانات.

وفي القانون المصري لم يواجه المشرع المصري بعد المشاكل القانونية المترتبة على حماية الوثائق الإلكترونية من خلال مواقع الإنترنت، كذلك لا توجد أحكام قضائية بمصر مماثلة لتلك الأحكام التي صدرت في كل من الولايات المتحدة الأمريكية وفرنسا التي تضفي على اختلاس المعلومات وتسريبها وفضح سريتها وصف السرقة أوخيانة الأمانة أوالاحتيال، إلا أنه وفر بعض الحماية من خلال نصوص قانون حق المؤلف، فورد بالمادة الثانية منه "تشمل هذه الحماية مؤلفي ... مصنفات الحاسب الآلي من برامج وقواعد بيانات وما يماثلها من مصنفات تحدد بقرار من وزير الثقافة وتعد هذه المصنفات من المصنفات الأدبية"، وتضيف المادة الرابعة من ذات القانون"، مع عدم الإخلال بحكم المادة 19 لا تشمل الحماية ... أولا - المجموعات التي تنتظم مصنفات عدة كمختارات الشعر والنثر والموسيقى وغيرها من المجموعات وذلك مع عدم الإخلال بحقوق كل مصنف... ومع ذلك تتمتع المجموعات سالفة الذكر إذا كانت متميزة بسبب يرجع إلى الابتكار أوالترتيب أوأي مجهود شخصي آخر يستحق الحماية".

ويتضح للباحث من النصين السابقين أن المشرع المصري كفل الحماية للوثائق من خلال برامج الحاسوب وقواعد البيانات وعدها من المصنفات الأدبية وأعطى لوزير الثقافة سلطة إضافة مصنفات أخرى تماثلها. .وقد فرض المشرع عقوبات مناسبة لتقليد المصنفات الأدبية ومن بينها برامج الحاسب وقواعد البيانات وفق المادة 47 من قانون حماية حق المؤلف.(رمضان، 2003)

وقد اختلف الرأي حول ذلك، فبينما ذهب البعض إلى القول بافتراض توافر القصد الجنائي، وأنه يقع على الجاني عبء إثبات حسن النية(لطفي، 2000)، والجريمة المشار إليها من الجرائم العمدية التي يقوم ركنها المعنوي بالقصد، ذهب البعض الآخر إلى أن هذه الجريمة تقوم بالقصد الجنائي العام، ويضيف البعض الآخر أن القول إن القصد الجنائي مفترض يتعارض مع صراحة النص (قايد، 1991) ومبادئ دستورية أساسية كقرينة البراءة، ومبدأ شخصية المسؤولية الجنائية، ويخلص إلى أنه يعد مرتكبا للجريمة المنصوص عليها بالمادة 47 من قانون حماية حق المؤلف من يقوم بتقليد موقع للإنترنت أوالتعديل أوالتحوير فيه دون موافقة صاحبه.

في القانون الأردني في هذا المجال خطا المشرع الأردني في عام 2001 خطوة تحسب له وذلك من خلال تعديل قانون العقوبات الأردني ليجرم اختراق شبكات الحاسوب وتخريبها وحماية الوثائق والمعلومات والبيانات وعدم تسريبها وذلك بموجب القانون رقم 54 لسنة 2001 (الجريدة الرسمية4467، 2000) المعدل لقانون العقوبات الذي أدخل تعديلا على المادة 148 من القانون الأصلي رقم 16 لسنة 1960 بالنص صراحة على تجريم "تعطيل سبل الاتصالات وأنظمة الحاسوب أواختراق شبكاتها أوالتشويش عليها أوتعطيل وسائط النقل أوإلحاق الضرر بها كليا أوجزئيا(قانون العقوبات الأردني رقم16، 1960).

كما خطا المشرع خطوة أخرى وذلك بإقراره نصا عاما في قانون المعاملات الإلكترونية المؤقت رقم (6) لسنة 2013 حيث نصت المادة 44 منه على أن "يعاقب كل من يرتكب فعلا يشكل جريمة بموجب التشريعات النافذة بوساطة استخدام الوسائل الإلكترونية مدة لا تقل ثلاثة سنوات وبغرامة لاتقل عن سنة الاف دينار ويعاقب بالعقوبة الأشد. إذا كانت العقوبات المقررة في تلك التشريعات تزيد

على العقوبة المقررة في هذا القانون في حال أفشى معلومات خاصة بالغير حصل عليها أثناء تسجيلها أوإرسالها بأي وسيلة من وسائل المعالجة المعلوماتية وكان من شأن إفشائها المساس بسمعة وخصوصيات صاحبها أوالغير".(قانون المعاملات الإلكترونية المؤقت رقم6، 2013)

هذا بالطبع إضافة إلى تجريم قرصنة برامج الحاسوب بموجب قانون حماية حق المؤلف رقم 22 لسنة 1992 وقانون الاتصالات رقم 13 لسنة 1995م، وحاليا هناك دراسة لا صدار قانون خاص باسم جرائم الحاسوب والانترنت حسب توصيات مجلس الوزراء الداخلية العرب.

بقي أن نشير إلى أن جرائم الحاسوب المرتكبة في الأردن لم تخرج بعيدا عن طورها التقليدي، أي استخدام الحاسوب كأداة لتنفيذ جرائم كالتزوير والتزييف أوالقرصنة، وقد تعلق معظمها ببطاقات الائتمان واحتيال عبر الإنترنت وقضايا اختراق)، إلا أن ذلك يشكل مؤشرا على إمكانية حدوث جرائم مستقبلية ذات أنماط غير تقليدية خطيرة كجرائم التخريب وتغيير البيانات وسرقة المعلومات والتي يكون الحاسوب هدفا فيها حيث تزيد احتمالية حدوث هذه الجرائم بازدياد الاعتماد على الحاسوب في شتى المجالات في المملكة، وبالتالي فإننا ندعوالمشرع الأردني إلى ضرورة الإسراع في إصدار تشريع جزائي عصري يعالج المشكلات القانونية الناجمة عن إساءة استخدام أجهزة الحاسوب والإنترنت. (رمضان، 2004)

ويعد تسريب الوثائق المحمية عبر الحاسوب جريمة الكترونية ولذلك فإن للجريمة الإلكترونية سواء أكانت تسريب وثائق الدولية الحكومية المحمية، أوتزويد الوثائق والبيانات عبر الحاسوب أوالمواقع الإلكترونية لذلك فإن للجريمة الإلكترونية أركان ثلاثة، على النحوالآتي: (الجبور، 2012)

- الركن الشرعي: وهوالصفة غير المشروعة للفعل، وتتمثل قاعدة التجريم والعقاب الجرائم الإلكترونيـة في مـا ورد الـنص عليـه في قـانون جـرائم أنظمـة المعلومـات الأردني.

- الركن المادي: وهوماديات الجريمة التي تبرز به إلى العالم الخارجي.

- الركن المعنوي: وهوالإرادة التي يقترن بها الفعل سواء في صورة القصد أوالخطأ.

وسأبحث الركنين المادي والمعنوي في الجرائم الإلكترونية وذلك في فرعين.

- الفرع الأول: الركن المادي في الجرائم الإلكترونية:

من المشكلات العملية التي تثيرهـا الجريمـة الإلكترونيـة طبيعـة الـركن المـادي في الجريمة الإلكترونية، ذلك أن مفهوم أومناط التجريم ينصب على نظام إلكتروني يسـاء استعماله أويتم اقتحامه على نحوغير مشروع، بما يكون لـذلك الاسـتعمال أوالاقتحـام من أثر مادي ملموس يظهر إمـا في صـورة تـدمير للمعلومـات، وهومـا يثـير إمكانيـة الإتلاف العمدي.

وتعتبر الجرائم الإلكترونية من أبرز أنواع الجرائم الحديثة التـي يمكـن أن تشـكل أضرارا جسيمة في ظل العولمة، فـلا غرابـة أن تعـد الجـرائم الإلكترونيـة - سـواء التـي تتعرض لها أجهزة الكمبيوتر أوالتـي تسـخر تلـك الأجهـزة في ارتكابهـا - مـن الجـرائم المستحدثة، حيث إن التقدم التكنولوجي الذي تحقق خلال السنوات القليلة الماضـية جعل العالم بمثابة قرية صغيرة، بحيث يتجاوز هذا التقدم بقدراته وإمكاناتـه أجهـزة الدولة الرقابية، بل إنه أضعف من قدراتها في تطبيق قوانينهـا، بالشـكل الـذي أصـبح يهدد أمنها وأمن مواطنيها.(إبراهيم، 2009)

إن محل جريمة تسريب الوثائق عبر الوسائل الإلكترونية قد يظهر بمظهرين أحدهما مادي والثاني معنوي، كما هوالحال بالنسبة للمعلومات فقد تكون في حالة انتقال أوموجودة في ذاكرة النظام الإلكتروني أي أنها في حالة غير مادية، والشكل الآخر أن تكون المعلومات متجسدة في صورة مادية جاء بتخزينها على دعامة إلكترونية، حتى أن المعلومات غير المادية بطبيعتها يمكن أن تخضع لأكثر من نص قانوني، وفقا لما إذا كانت في شكل مادي أوغير مادي، وفي الشكل الأخير يوجد لها أكثر من نص قانوني يمكن أن تخضع له، مثال ذلك اعتبارها مصنف أدبي مما يثير مشكلة تعدد الأوصاف القانونية على ذات المحل(إبراهيم، 2009).

وللمنقولات، أوالسرقة وذلك عن طريق إساءة استعمال بطاقات الائتمان، أويثير شبهة التزوير والتسريب عن طريق التلاعب في بيانات الحاسب الآلي.

إن السلوك الإجرامي في جريمة تسريب الوثائق المحمية الإلكترونية يرتبط دائما بالمعلومة المخزنة على الحاسب الآلي، أوتلك التي يتم إدخالها للحاسب الآلي، وصعوبة المشكلة أن السلوك الإجرامي قد يتحقق بمجرد ضغط زر في الحاسب فيتم تدمير النظام المعلوماتي أوحصول التزوير أوالسرقة عن طريق التسلل إلى نظام أرصدة العملاء في البنوك أوإساءة استعمال بطاقات الائتمان(معاشي، 2011).

إن السلوك الإجرامي بوصفه عنصرا في الركن المادي في الجريمة التقليدية يتم رؤيته رؤى العين والتأكد منه كفعل القتل أوالسرقة أوالتزوير، ولكن صعوبة الجريمة الإلكترونية، والركن المادي فيها خاصة أن الجريمة ترتكب عن طريق معلومات تتدفق عبر نظم الحاسب الآلي لا يمكن الإمساك مادية بها، تماما مثل التيار الكهربائي الذي يسري في توصيلة دون أن تراه، لذلك يتعين تحليل السلوك الإجرامي في الجريمة الإلكترونية خاصة ما يتعلق فيها بفكرة المال في جرائم الاعتداء على المال

العـام أوالخـاص، كـما لا بـد مـن العـرض الصـور السـلوك الإجرامـي في الجريمـة الإلكترونية(حجازي، 2007).

إن السـلوك المـادي أوالنشـاط في جريمـة تسريـب الوثـائق المحميـة الحكوميـة الإلكترونية يتطلـب وجـود بيئـة رقميـة وجهـاز كمبيـوتر واتصـال بشـبكة الإنترنـت، ويتطلب أيضا معرفة بداية هذا النشاط والشروع فيـه ونتيجتـه، فعـلى سـبيل المثـال يقوم مرتكـب الجريمـة بتجهيـز الكمبيـوتر لـكي يحقـق لـه حـدوث الجريمـة، فيقـوم بتحميل الحاسب ببرامج اختراق، أوأن يقوم بإعداد هذه البرامج بنفسه، كما يمكـن أن يقوم بجريمة إعداد برامج فيروسات تمهيدا لبثها لمنع الدخول إلى الوثائق، ولـيس كـل جريمـة تسـتلزم وجـود أعـمال تحضـيرية، وفي الحقيقـة يصـعب الفصـل بـين العمـل التحضيري والبدء في النشاط الإجرامي في جرائم الكمبيوتر والإنترنت – ومنهـا جريمـة تسريب الوثائق المحمية حتى ولوكان القانون لا يعاقب على الأعمال التحضـيرية - إلا أنه في مجال تكنولوجيا المعلومات، الأمر يختلف بعـض الشيء، فشراء بـرامج اخـتراق، ومعدات لفك الشفرات وكلمات المـرور، وحيـازة صـور دعـارة للأطفـال، فمثـل هـذه الأشياء تمثل جريمة في حد ذاتها. (حجازي، 2007)

ويرى الباحـث أن النشـاط أوالسـلوك المـادي في الجريمـة الإلكترونيـة يعـد محـلا لتساؤلات عديدة فيما يتعلق ببدايته أوالشروع في ارتكاب الجريمة، ومثل هذا النشاط يختلف عما هوالحال عليه في العالم المـادي، فارتكـاب الجريمـة عـبر الإنترنـت يحتـاج بالضرورة إلى منطق تقني، وبدونه لا يمكن للشخص حتـى الاتصـال بالإنترنـت، سـواء كان بقصد ارتكاب جريمة أم لمجرد التصفح أوالـدخول في الاتصـال المبـاشر كالمحادثـة وغيرها.

وهذا السلوك أوالنشاط المادي الإيجابي الممثل في المنطق التقني يجعل جريمة تسريب الوثائق المحمية عبر الإنترنت طابع موحد بالضرورة، فهي تباشر من حيث السلوك أوالنشاط المادي فيها، كأحد ذات عناصر الركن المادي يضاف إلى فلسفة الركن المادي في الجريمة، مثل هذا الأمر تداركه المشرع الأردني حين نص على جرائم تسريب الوثائق المحمية أونقل المعلومات والبيانات وتزويرها يمكن أن ترتكب عبر الكمبيوتر، ففي مثل هذه النصوص نجد المشرع الأردني يقرر صراحة عبارة ... "إذا ارتكبت الجريمة باستخدام نظام معلومات أوالشبكة المعلوماتية ..." أوعبارة "... باستخدام المعالجة الآلية للبيانات" ففي مثل هذه الحالات يكون المشرع الأردني مدركا لمسألة الشروع في ارتكاب جريمة تسريب الوثائق المحمية عبر الشبكة المعلوماتية المرتبطة بالإنترنت(قانون جرائم أنظمة المعلومات الأردني رقم(30)، 2010م).

لذلك يعد الدفع بعدم وجود قدرات تقنية حال الاتهام بارتكاب جريمة تسريب الوثائق المحمية عبر الإنترنت من الدفوع الموضوعية الجوهرية التي تلتزم محكمة الموضوع بالرد عليه تفصيلا، وإلا عاب حكمها عيبا في التسبيب بما يسمح بقبول نقضه، ولقد جعلت الطبيعة الموحدة للجريمة عبر الإنترنت، من حيث اتحاد جميع أشكالها المادية في ضرورة استخدام الآلة كوسيط إلى ارتكابها أن اتصفت هذه الجريمة بالضرورة بالطابع التقني. (إبراهيم، 2009)، ولكي يتوافر الركن المادي في جريمة تسريب الوثائق المحمية الإلكترونية، فلا بد من حصول النتيجة الإجرامية على أن ترتبط بالسلوك الإجرامي بعلاقة سببية.

- **الفرع الثاني: الركن المعنوي للجريمة الإلكترونية:**

الركن المعنوي هوالحالة النفسية للجاني، والعلاقة التي تربط بين ماديات الجريمة وشخصية الجاني، فالركن المعنوي هوالمسلك الذهني أوالنفسي للجاني باعتباره محور القانون الجنائي، ذلك أنه في إطار هذا الركن تتوافر كافة مقومات المسؤولية الجنائية، من علم وإرادة آثمة وقصد جرمي مع إقرار حق الدولة في العقاب الذي يبني على هذه المقومات، لذلك يمكن تعريف الركن المعنوي بأنه: العلاقة التي تربط بين ماديات الجريمة وشخصية الجاني مرتكبها، وهذه العلاقة هي محل الأذناب في معنى استحقاق العقاب، ومن ثم يوجه إليها لوم القانون وعقابه(الجبور، 2010). ويتوفر القصد الجنائي في جريمة تسريب الوثائق المحمية عبر الوسائل الإلكترونية في حق الجاني في حالات ثلاثة، هي: (حسني، 2011)

الأولى: إذا كان الجاني يتوقع ويريد أن يترتب على فعله أوامتناعه حدوث الضرر أووقوع الخطر الذي حدث والذي يعلق عليه القانون وجود الجريمة.

الثانية: إذا نجم عن الفعل أوالامتناع ضرر أوخطر أكثر جسامة مما كان يقصده الفاعل، وهي حالة جواز القصد التي ينص عليها القانون صراحة على إمكان ارتكابها بهذا الوصف.

الثالثة: الحالات التي يعزى فيها القانون الفعل إلى الفاعل نتيجة لفعله أوامتناعه، أي حالات يفترض فيها القانون توافر القصد الجنائي لدى الجاني افتراضاً، وهومستمد من أنه طالما أن النتيجة الجسيمة التي تحققه نشأت عن فعل الجاني، فمقتضى ذلك أن هذا الفعل كان صحيحا لإحداثها، ولكونه كذلك فإن الجاني يجب أن يتحمل نتائجه، توقعها أم لم يتوقعها.

إن توافر الركن المعنوي في الجرائم الإلكترونية يعد مـن الأمـور الهامـة في تحديـد طبيعة السلوك المرتكب وتكييفه لتحديد النصوص التي يلزم تطبيقها، إذ بدون الركن المعنوي لن يكون هناك سوى جريمة واحدة هي جريمة التسريب غير المشروع.

إن القضاء الأمريكي لم يستقر عـلى حـال بالنسـبة لـبعض الجـرائم التـي ترتكـب باستخدام الإنترنت مثل جريمة تسريب الوثائق المحمية من حيث مدى تحديد ما إذا كانت تتطلب قصدا عاما أم خاصة، فـذلك لا يمـانع في تطلـب قصـد جنـائي خـاص في جريمة التهديد، إلا أنه يقر من جديد أنه يكفي بالقصد العام عن ذات الجريمـة، كـما هوالشأن في جريمة التهديد بالبريد الإلكـتروني وعـبر المجموعـات الإخباريـة وفـق مـا هومقرر في القسم والقصد العام فيها، بينما يتم استدلاء معالمه من النظرة الموضوعية إلى السلوك الشخصي مـن مجموعـة الظـروف المحيطـة بالجريمـة بمـا في ذلـك فحـص الحالة العقلية لمرتكب الجريمة. (إبراهيم، 2009)

أما في القضاء الفرنسي فإن منطق سوء النية يكتسح النصوص التـي تطبـق بشـأن الإنترنت، حتى أن هذه الجرائم لا يمكن أن تـدخل حيـز التطبيـق مـا لم يتـوافر سـوء النية في منطق القصد الخاص وإرادة الإضرار، ومن ذلـك مـا هـومقرر في المـادة (15-226 عقوبات فرنسي جديد) التي تشترط سوء النية حـين وجـود عـدوان عـلى البريـد الإلكتروني، وبما يجعل ذلك بالضرور متطابقا مع ما هومقرر في المـادة (**L 32-1 II.5**) من تقنين البريد والاتصالات الصادر بالقـانون المـؤرخ 1996/7/26م التـي تلـزم وزيـر الاتصالات الفرنسي بالسهر على مبدأ احترام سرية الاتصالات".(موسى، 2010)

"كذلك الحال لدى المشرع البريطاني، فالركن المعنوي في الجريمة الإلكترونية ومنها جريمـة تسريـب الوثـائق المحميـة يتطلـب أن تـنصرف إرادة الجـاني نحوالـدخول إلى البيانـات أوالمعطيـات المخزنـة في أي حاسـوب، إذ جـرم المشرع البريطـاني الـدخول

غير المصرح به للنظـام الإلكـتروني بموجـب المـادة الأولى مـن قـانون إسـاءة اسـتخدام الحاسوب البريطاني لعـام 1990م، وكـذلك جـرم الـدخول غـير المصرح بـه إلى النظـام الإلكتروني بهـدف ارتكـاب جريمـة أخـرى بموجـب المـادة الثانيـة مـن نفـس القـانون (الرواشدة، 2009).

- الفرع الأول: أطراف الجريمة الإلكترونية:

لا بد للجريمة الإلكترونية كغيرها من الجرائم أن يكون لها فاعل ومجني عليه.

أولا: الفاعل في الجريمة جريمة تسريب الوثائق المحمية الإلكترونية: (الشوا، 2011)

بالإضافة إلى الشروط العامة الواجب توافرها في مرتكب الجريمة الإلكترونيـة مـن سلوك منحرف وعلم وإرادة في نتائج هذا السلوك، ينبغي أن يكون هذا الشخص على درجة معينة من العلم والخبرة العملية في شؤون عالم الحاسـوب وتقنيـة المعلومـات، وقد سماه البعض بالمجرم الإلكتروني أوالمجرم المعلوماتي.

وبهذا المعنى لا يتصور أن يكون الجاني في جريمـة تسريـب الوثـائق المحميـة عـبر الوسائل الإلكترونية إلا شخصا طبيعيا ذا أهليـة وقـدرة عـلى أن يكـون محـلا لتوقيـع العقوية وهوالأمر الذي لا يتصور حدوثه إلا بالنسبة للشخص الطبيعي دون الشـخص المعنوي(سلامة، 2017)، كما لا يتصور أن يكون الجاني هنا إلا شخصاً ذا خـبرة ودرايـة في علم الحاسوب سـواء أكـان مسـتخدمة أومبرمجـة أومجـرد هـاوأومحترف الجـرائم الحاسوب وتقنية المعلومات.

هذا ويتميز الفاعل في الجريمة الإلكترونية مثل جريمـة تسريـب الوثـائق المحميـة عبر الوسائل الإلكترونية بعـدد مـن السـمات والخصـائص، هـي: أنـه يتمتـع بالمهـارة

والمعرفة والذكاء، كما أنه إنسان اجتماعي، كذلك يعمل على تبرير ارتكاب جريمته وفي الوقت ذاته يتولد لديه شعور بالخوف من كشف جريمته، كما أن الفاعل في هذه الجريمة يتمتع بالسلطة تجاه النظام الإلكتروني(الزيدي، 2009).

ثانيا: المجني عليه في الجرائم الإلكترونية:

إذا كان الغالب الأعم بأن مرتكب الجريمة الإلكترونية يكون شخصا طبيعية أومؤسسة حكومية، فإن المجني عليه هنا هوبالغالب الأعم شخص معنوي كالبنوك والشركات الكبرى والمؤسسات الحكومية والوزارات والمنظمات والهيئات المالية، وغيرها من الأشخاص الاعتبارية التي تعتمد في إنجاز أعمالها على الحواسيب(قاسم، 2010).

حيث يصعب تصور وقوع جريمة تسريب الوثائق المحمية عبر الوسائل الإلكترونية بالنسبة للأفراد العاديين وإن كان ذلك غير مستبعد، إذ قد يتعرض الفرد العادي لشكل من أشكال الجريمة الإلكترونية فيما إذا كان من بين الأشخاص الذين يحفظون أسرارهم التجارية وأعمالهم وشؤونهم داخل الحاسوب الخاص به، ونبغي لقيام الجريمة الإلكترونية في هذا الفرض أن يكون الشخص العادي (المجني عليه) هنا من بين الأشخاص الذين قد ينجذب إليهم الجناة كأن يكون ذا منصب سياسي رفيع أورجل أعمال مرموق أوصاحب شهرة عالمية في قطاع من القطاعات الاقتصادية أوالاجتماعية العسكرية(الدسوقي، 2003).

وعلى الرغم من إمكانية تعرض الجميع للجريمة الإلكترونية سواء أكانوا أشخاصا معنوية أوطبيعية إلا أن معظم جريمة تسريب الوثائق المحمية عبر الوسائل الإلكترونية ترتكب من أجل أمرين وهما: المال والمعلومات، جريمة تسريب الوثائق المحمية عبر الوسائل الإلكترونية أوالحقد على الجهة الحكومية أوأشخاص

بعينهم وبالتالي يمكن القـول بـأن الغالبيـة العظمـى مـن المجنـي علـيهم في الجـرائم الإلكترونية هم إما مؤسسات مالية كالبنوك والمصارف وشركات الصرافة، وإما شركـات المعلومات بصرف النظر عن نوع هذه المعلومات أوقيمتها إذ قد تكون بالغة الأهمية كالمعلومات العسكرية والمخابراتية، وقد تكون معلومات رياضية أوفنيـة أواجتماعيـة بسيطة(الخزاعلة، اخوارشيدة، 2021).

إن تحديد نطاق خاص يضم كافة فئات المجني عليهم في الجرائم الإلكترونية يعد أمرا صعبا بسبب حقيقة أن المجني عليهم في هذه الجرائم غالبا من يكتشفونها بعـد حصولها، الأمر الذي دفعهم في غالب الأحيان إلى السكوت والإذعان لها وتفضيل هـذا الموقف السلبي عن القيام بالتصريح عن تعرض أجهـزتهم ومعلومـاتهم التـي يفـترض فيها الأمان والسرية إلى الدخول غير المشروع والانتهاك، وهوالأمر الـذي يشـكل بحـد ذاته سببا في ازدياد معدل جريمة تسريب الوثـائق المحميـة عـبر الوسـائل الإلكترونيـة وصعوبة اكتشافها أوالحد منها، ومن ثم كثرة مشكلاتها ثم الصعيد القانوني والعمـلي. (الخوالدة، 2012)

- الفرع الثاني: محل الجريمة الإلكترونية:

لعل الجرائم الإلكترونية تستهدف أحد أوكل العناصر التالية: (الملط، 2006)

أولا: الوثائق والمعلومات:

تشمل جريمة تسريب الوثائق المحمية عـبر الوسـائل الإلكترونيـة في هـذه الحالـة سرقة أوتغيير أوحذف المعلومـات، فمـثلا في حالـة النشـاط الجرمـي الـذي يسـتهدف اختراق بريد إلكـتروني والعبـث بمحتوياتـه، أوسرقـة المعلومـات المخزنـة في موقـع مـا والاستفادة منها بما يحمل في طياتـه بعضـا مـن انتهـاك الخصوصـية وحقـوق الملكيـة الفكرية وأنماطا جرمية أخرى.

ثانيا: الأجهزة:

تشمل الجرائم الإلكترونية في هذه الحالة تعطيل أجهزة الكمبيوتر أوتخريبها عبر إرسال الفيروسان أوالبرامج التي تحوي أنظمة هجومية مما يسبب تلفا في أنظمة الكمبيوتر يؤدي لشلل كل الأنشطة المرتبطة بهذا الجهاز أوالأنظمة المرتبطة به.

"فمثلا في الولايات المتحدة الأمريكية أصدر مكتب التحقيقات الفيدرالي الأمريكي إنذار عامة يحذر مستخدمي الإنترنت من مخاطر تسريب الوثائق المحمية عبر الوسائل الإلكترونية جديدة، تنطوي على فخ، يدفع المستخدمين إلى الكشف عن بيانات حساباتهم المالية الشخصية، ليصار لاحقا إلى السطوعليها". "وحذرت دائرة شكاوى جرائم الإنترنت التابعة للمكتب الفيدرالي، من ظهور مجموعة من الرسائل الإلكترونية التي تزعم أن المتلقي قد قام بعمليات شراء البضائع عبر الشبكة، وتستدرجه للكشف عن بيانات حساباته، وقالت الدائرة إن نموذجين من تلك الرسائل تم رصدهما، تدعي الأولى أن المتلقي قد عقد طلبية لشراء جهاز كمبيوتر عبر الشبكة، وتطلب منه في حال عدم رغبته بإتمام الطلبية الدخول إلى وصلة البيانات الشخصية لإلغائها، وسيجد متصفح البريد الإلكتروني الذي يدخل تلك الوصلة معلومات شخصية حول حساباته المالية، يتوجب عليه الكشف عنه الإلغاء عملية الشراء المزعومة، وبذلك يحقق أصحاب تلك الرسائل هدفهم، أما النموذج الثاني فيتضمن بيان كشف مشتريات مرسلة كملف **PDF**، تحتوي على فيروس يتسلل إلى جهاز الكمبيوتر الشخصي للمتلقي، ما أن يقوم بالدخول وتشغيل الرسالة القراءتها". (تمام، 2009)

ثالثا: الأشخاص أوالجهات:

تهدف فئة كبيرة من الجرائم الإلكترونية أشخاص أو جهات بشكل مباشر كالتهديد أو الابتزاز أو السرقة أوممارسة الفاحشة. فمثلا سرقة المال عبر الإنترنت باستخدام أرقام البطاقات مصرفية تعود للغير، أو الحض على الفجور وممارسة الفاحشة مع قاصر عبر الإنترنت، أو الإرشادات التي تحمل في طياتها تعليمات إرهابية كلها موجهة ضد أشخاص أو جهات بعينها.(الخزاعلة وآخرون، 2016)

أما الآليات التي تنفذ بها جريمة تسريب وثائق الدولة المحمية عبر الوسائل الإلكترونية فقد تكون الآليات إحدى الوسائل الآتية: (الجهيني، 2015)

قد تكون شبكة الإنترنت هدفا للجريمة، وذلك كما في حالة الدخول غير المصرح به إلى أنظمة البيانات في مواقع إلكترونية معينة تسريب وثائق ومعلومات سرية وخطيرة ومحمية ولتدمير المعطيات أوالاستيلاء على البيانات المخزنة أو المنقولة عبر النظم، أو أن يتم إخفاء هذا النشاط الجرمي بإعادة إنتاج وطرح هذه البيانات عبر نفس الشبكة ولمشتركين يستخدمون الدفع عبر الإنترنت وهكذا، وهذا ما أكده المشرع الأردني في المادتين (3، 4) من قانون جرائم أنظمة المعلومات.

قد تكون شبكة الإنترنت أداة الجريمة لارتكاب جرائم إلكترونية عبرها فقط، كما في حالة استغلال الإنترنت للاستيلاء على الأموال بإجراء تحويلات غير مشروعة أو استخدام التقنية في عمليات التزييف والتزوير، أو استخدام التقنية في الاستيلاء على أرقام بطاقات ائتمان وإعادة استخدامها والاستيلاء على الأموال بواسطة ذلك، ومن ثم الدخول في عمليات دفع إلكترونية وشراء عبر الإنترنت لإخفاء المصدر الحقيقي غير المشروع للأموال القذرة، وقد نص المشرع الأردني على تجريم مثل هكذا حالات بموجب المادة (6) من قانون جرائم أنظمة المعلومات. ولعل أبرز ما يمكن أن نشاهده في هذا الإطار أنشطة غسل الأموال التي تتم عبر الإنترنت وما يرتبط بها من

عمليات معقدة ظاهرها التجارة الإلكترونيـة والتعاقـد عـبر الإنترنـت وباطنهـا إخفـاء المصادر الحقيقية غير الشرعية للأموال (عبد اللـه، 2011).

وقد تكون شبكة الإنترنت في البيئة التي ينموفي رحمها الإجـرام المعلومـاتي وذلـك كما في إبرام اتفاقيات الترويج المخدرات وأنشطة الشبكات الإباحية والإرهابية وغسل الأموال.

أما من حيث دور شبكة الإنترنت في اكتشاف جريمة تسريب الوثائق والمعلومـات والبيانات عبر الوسائل الإلكترونية التي تتم عبر الشبكة، فـإن الإنترنـت يسـتخدم الآن على نطاق واسع في تتبع الجرائم، عوضـا عـن أن جهـات إنفـاذ القـانون تعتمـد عـلى النظم التقنية في إدارة المهام من خلال بناء قواعـد البيانـات المشـتركة وأطـر التعـاون الدولي، ومع تزايد نطاق الجرائم الإلكترونية، واعتماد مرتكبيهـا عـلى وسـائل التقنيـة المتجددة والمتطورة، فإنه أصبح لزاما استخدام نفس وسائل الجريمة المتطورة للكشف عنها، من هنا تلعب شبكة الإنترنت ذاتها دورا رئيسيا في كشـف الجـرائم الإلكترونيـة والإنترنت وتتبع فاعليها، بل وإبطال أثرها.(الرومي، 2013)

إن كثرة وسائل التواصل الاجتماعي في وقتنا الحاضر وتنوعها وجدت احـتمالا قـل نظيره في ارتكاب الجرائم الإلكترونية، ولعل "تويتر" يعد من أبرز هذه الوسـائل الـذي اكتسح مجال العالم الافتراضي بعد أن اقتنع مرتكبي الجـرائم الإلكترونيـة بأنـه وسـيلة فعالــة الارتكــاب هــذه الجــرائم وذلــك مــن خــلال تغريــداتهم وســهولة كتابتهــا وإرسالها(الحسيني، 2013).

هذا ويجب عدم الخلط بين دور الوسائل الإلكترونية في الجريمة الذي يكـون إمـا الهدف المباشر للاعتداء، أووسيلة الاعتداء، أوتكون بيئة ومخزن للجريمـة، وبـين محـل الجريمة السابق بيانه الذي يكون دائما المعلومات والأجهزة والأشـخاص والهيئـات إمـا بذاتها أوبما تمثله.

المبحث الثاني :عقوبة الجريمة الإلكترونية أنموذج نشر وتسريب الوثائق المحمية

جرمت المادة (15) من قانون حماية أسرار ووثائق الدولة رقم (50) لسنة 1971 وتعديلاته، كل موظف عام قام بإفشاء أسرار الدولة والوثائق المحمية وفرض عقوبة على بالأشغال الشاقة لمده تصل إلى عشر سنوات.(قانون حماية أسرار ووثائق الدولة رقم (50)، 1971)

وقد وسعت المادة (16) من قانون العقوبات نطاق الحماية على أسرار ووثائق الدولة، حيث امتد خطر إفشاء الأسرار والمعلومات إلى مرحله ما بعد انتهاء العلاقة القانونية بين الموظف والإدارة العامة والمتمثلة بالتقاعد والاستقالة والإقالة.

ويرى الباحث أن تسريب الوثائق الرسمية سواء أكان ذلك التسريب بالأسلوب التقليدي أم عن طريق وسائل التواصل الاجتماعي والأدوات الإلكترونية بأنه تصرف غير مسؤول، يمس الانتظام العام في الجهاز الإداري الحكومي، ويترتب عليه عقوبة تأديبية قد تصل إلى الاستغناء عن خدماته وعقوبة الجزائية تصل إلى السجن عشر سنوات مع الأشغال الشاقة.

إن تفشي ظاهرة تسريب الوثائق المحمية عبر الوسائل الإلكترونية تعد جريمة الكترونية، حيث أن التساهل في الإفصاح عنها يؤدي إلى الاختلال في الانتظام العام، للجهاز الإداري الحكومي في الدولة الذي يرتبط بالتأثير على ثقة الجمهور بالوظيفة العامة ويؤدي بالنتيجة إلى الإخلال بسير المرافق العامة بانتظام واطراد، وان علاج مثل هذه الظاهرة والحلول لها تبدا من خلال الحق في الحصول على المعلومات، وتطبيق مبدأ الإفصاح ألاستباقي ومبدأ لكشف الأقصى عن المعلومات.

وعند البحث في قانون حماية أسرار ووثائق الدولة رقم (50) لسنة 1971، نرى ان القانون قد عاقب كل من يقوم بنشر وثائق الدولة المحمية بما يلي: .(قانون حماية أسرار ووثائق الدولة رقم (50)، 1971)

نصت المادة (14) من دخل أوحاول الدخول إلى مكان محظور قصد الحصول على أسرار أوأشياء أووثائق محمية أومعلومات يجب ان تبقى سريه حرصا على سلامه الدولة عوقب بالأشغال الشاقة المؤبدة، وإذا كانت الدولة الأجنبية عدوه فتكون العقوبة إعدام.

أما المادة (15) من القانون ذاته فقد نصت على ما يلي: .(قانون حماية أسرار ووثائق الدولة رقم (50)، 1971)

أ) من سرق أسرار أوأشياء أووثائق أومعلومات كالتي ذكرت في المادة (14) واستحصل عليها عوقب بالأشغال الشاقة المؤقتة لمده لا تقل عن 10 سنوات.

ب) اذا اقترفت الجناية لمنفعة الدولة أجنبية كانت العقوبة بالأشغال الشاقة المؤبدة وإذا كانت الدولة أجنبية عدوه فتكون العقوبة الإعدام.

أما المادة رقم (16) فقد نصت على ما يلي:

أ- من وصل إلى حيازته أوعلمه أي سر من الأسرار أوالمعلومات أوأية وثيقة محمية بحكم وظيفته أوكمسؤول أوبعد تخليه عن وظيفته أومسؤولية لأي سبب من الأسباب فابلغها أوأفشاها دون سبب مشروع عوقب بالأشغال الشاقة المؤقتة مدة لا تقل عن عشر سنوات.

ونصت المادة (4) من قانون الجرائم الإلكترونية الأردني رقم (27) لسنة 2015:"يعاقب كل من ادخل أونشر أواستخدم قصداً برنامجا عن طريق الشبكة المعلوماتية أوباستخدام نظام معلومات لإلغاء أوحذف أوإضافة أوتدمير أوإفشاء

أوإتلاف أوحجب أوتعديل أوتغيير أونقل أونسخ أوالتقاط أوتمكين الآخرين من الاطلاع على بيانات أومعلومات أوإعاقة أوتشويش أوإيقاف أوتعطيل عمل نظام معلومات أوالوصول اليه أوتغيير موقع الكتروني أوإلغائه أوإتلافه أوتعديل محتوياته أوأشغاله أوانتحال صفته أوانتحال شخصية مالكه دون تصريح أوبما يجاوز أويخالف التصريح بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة وبغرامة لا تقل عن (200) مائتي دينار ولا تزيد على (1000) ألف دينار"(قانون الجرائم الإلكترونية الأردني رقم (27)، 2015).

ويعتقد الباحث أن المادة (4) من قانون الجرائم الإلكترونية الأردني رقم (27) لسنة 2015 جاءت لتقطع الطريق على كل من تسول له نفسه إنشاء أي برنامج الكتروني يتم من خلاله نشر أوتسريب أوالمساعدة في نشر أوتسريب أي وثيقة حكومية محمية.

ونصت المادة (12) من القانون ذاته على ما يلي:(قانون الجرائم الإلكترونية الأردني رقم (27)، 2015)

يعاقب كل من دخل قصداً دون تصريح أوبما يخالف أويجاوز التصريح إلى الشبكة المعلوماتية أونظام معلومات باي وسيلة كانت بهدف الاطلاع على بيانات أومعلومات غير متاحة للجمهور تمس الأمن الوطني، أوالعلاقات الخارجية للمملكة، أوالسلامة العامة، أوالاقتصاد الوطني بالحبس مدة لا تقل عن أربعة أشهر وبغرامة لا تقل عن (500) خمسمائة دينار ولا تزيد على (5000) خمسة آلاف دينار.

إذا كان الدخول المشار اليه في الفقرة (أ) من هذه المادة، بقصد إلغاء تلك البيانات، أوالمعلومات، أوإتلافها، أوتدميرها، أوتعديلها، أوتغييرها، أونقلها،

أونسخها، أوإفشائها، فيعاقب الفاعل بالأشغال الشاقة المؤقتة وبغرامة لا تقل عن (1000) ألف دينار ولا تزيد على (5000) خمسة آلاف دينار.

يعاقب كل من دخل قصداً إلى موقع الكتروني للاطلاع على بيانات أومعلومات غير متاحة للجمهور تمس بالأمن الوطني، أوالعلاقات الخارجية للمملكة، أوالسلامة العامة، أوالاقتصاد الوطني بالحبس مدة لا تقل عن أربعة أشهر وبغرامة لا تقل عن (500) خمسمائة دينار.

وعند المقارنة بين المواد المتعلقة بتسريب أونقل أوالاطلاع على الوثائق أوالبيانات المحمية ولا التي اطلق عليها قانون الجرائم الإلكترونية بأنها غير متاحة للجمهور وتمس بالأمن الوطني أوالعلاقات الخارجية للمملكة أوالسلامة العامة أوالاقتصاد الوطني، نرى ان العقوبة في كلي القانونين كانت على النحوالآتي: .(قانون حماية أسرار ووثائق الدولة رقم (50)، 1971)

في قانون حماية أسرار ووثائق الدولة رقم 50 لسنة 1971 واصلت عقوبة إفشاء أونقل أسرار وتسليم الوثائق المحمية إلى عقوبة الأشغال الشاقة المؤقتة لمده لا تقل عن عشر سنوات في حال سرقه أسرار أوأشياء أووثائق أومعلومات عن محمية.

وتصل العقوبة إلى الإعدام في حال كانت الدولة المفشى أوالمنقول أوالمسرب لها الأسرار أووثائق الدولة، دولة عدوه في قانون حماية أسرار ووثائق الدولة رقم 50 لسنة 1971 كل من دخل أوحاول الدخول إلى مكان محظور قصد الحصول على أسرار أوأشياء أوتسريب وثائق محمية أومعلومات يجب ان تبقى سريه حرصا على سلامه الدولة. .(قانون حماية أسرار ووثائق الدولة رقم (50)، 1971)

في قانون الجرائم الإلكترونية رقم (27) لسنة 2015 تصل العقوبة إلى ستة ولا تقل عن ثلاثة أشهر وبغرامه لا تقل عن 200 دينار ولا تزيد عن 5000 دينار كل من أفشى أوسرب أونقل أوتطلع على بيانات أومعلومات غير متاحة للجمهور الاطلاع عليها.

وبالمقارنة نرى أن قانون حماية أسرار ووثائق الدولة رقم 50 لسنة 1971 قد شدد على العقوبة بسبب الظروف السياسية التي كانت تمر بها المملكة الأردنية الهاشمية في تلك الفترة، وبسبب وجود صراعات عربيه- إسرائيلية، وأردنية- إسرائيلية من جهة أخرى بينما نرى ان الوسائل الإلكترونية الآن أصبحت متاحة للجميع بكل يسر وسهوله، ولا تستطيع الدولة ان تمنع الناس من الاطلاع على الوثائق المسربة بأي حال من الأحوال وذلك بسبب وجود برامج الكترونية تعمل على الاطلاع على تلك المعلومات أوالوثائق التي تخص الدولة من خلال اختراق البرامج الأمنية المصممة لحمايتها. .(قانون حماية أسرار ووثائق الدولة رقم (50)، 1971)

وما زالت الأردن تعمل بقانون حماية أسرار ووثائق الدولة رقم 50 لسنة 1971 إلى جانب قانون الجرائم الإلكترونية الأردني رقم (27) لسنة 2015، والملاحظ أن قانون حماية أسرار ووثائق الدولة رقم 50 لسنة 1971 يحتاج إلى تعديلات ضرورية بما يتلاءم مع مقتضيات قانون ضمان الحق في الحصول على المعلومات وبما يضمن حقوق الأفراد بالحصول على المعلومات بصوره شفافة وبما يضمن عدم استثناء معلومات واسعة من هذا الحق علاوة على ان العصر الذي يعيش هوعصر الوسائل الإلكترونية .

المبحث الثالث: الآثار القانونية والأمنية والاجتماعية للجريمة الإلكترونية (أنموذج نشر وتسريب الوثاق الرسمية الحكومية)

شهد العالم في الآونة الأخيرة ظاهرة غير معهودة تتمثل بتداول ونشر مضامين صور ووثائق حكومية يفترض بها السرية والتداول الداخلي المحدود، ووصل الأمر في بعض الأحيان لتداول وثائق رسمية مصنفه بالسرير جدا ومحدود الاطلاع وحتى من بعض الدوائر السيادية والأمنية الحساسة كذلك، لا بل وصل الأمر إلى استخدام سلك الوثائق عبر وسائل التواصل الاجتماعي والانترنت في فضح الممارسات الحكومية لبعض الدول أوغير القانونية أوغير الأخلاقية، في الوقت الذي اعتبرت فيه بعض القوى أن ذلك يعتبر جزءا من مفهوم الشفافية وحق الحصول على المعلومات وحق الاطلاع على أعمال الإدارة العامة، وخاصة في ظل تكتم الأنظمة السياسية على معظم المعلومات واحتكارها وعدم تفعيل قانون الحصول على المعلومات، حيث ان تلك الممارسات كان لها آثار قانونية أمنية واجتماعية في تسريب تلك الوثائق .

الآثار القانونية للجرائم الإلكترونية من خلال تسريب وثائق الرسمية الحكومية:

في كثيرٍ من الدول الديمقراطية هنالك مفهوم يعرف بالمُنذِر (**Whistle Blower**) وهوأن يقوم شخص ما بفضح عمل غير قانوني أوغير أخلاقي يتم ممارسته في مكان عمله، بحيث يتم حماية ذلك الشخص ضمن برنامج حماية الشهود، وذلك بهدف تحفيز الناس على كشف جوانب القصور والمخالفات التي تحدث في مؤسسات الدولة والشركات بدون التوجس من العواقب التي قد تلحق بالشخص المُنذِر بسبب فضحه لملفات معينة.(البناء، 2011)

لذا فإن الآثار القانونية لتسريب وثائق الدولة عبر الوسائل الإلكترونية كانت على النحوالآتي:

يعتبر الدخول إلى الوسائل الإلكترونية بقصد نقل أوتسريب الوثائق المحمية دخول غير قانوني غير مصرح به، لذا فإن المشرع الأردني جاء بنصوص تكفل تجريم فعل الدخول والبقاء غير المصرح به لنظام المعلومات، حيث نصت المواد من (3) إلى (11) من قانون جرائم انظمه المعلومات المؤقت لسنة 2010 والمعدل في عام 2015 ما يلي:

أ- من دخل قصداً موقعاً الكترونيا أونظام معلومات بأي وسيلة دون تصريح أوبما يخالف أويجاوز التصريح، يعاقب بالحبس مدة لا تقل عن أسبوع ولا تزيد على ثلاثة أشهر أوبغرامة لا تقل عن (100) مائة دينار ولا تزيد على (200) مائتي دينار أوبكلتا هاتين العقوبتين.

ب- إذا كان الدخول المنصوص عليه في الفقرة (أ) من هذه المادة بهدف إلغاء أوحذف أوإضافة أوتدمير أوإفشاء أوإتلاف أوحجب أوتعديل أوتغيير أونقل أونسخ بيانات أومعلومات أوتوقيف أوتعطيل عمل نظام معلومات أوتغيير موقع الكتروني أوإلغائه أوإتلافه أوتعديل محتوياته أوأشغاله أوانتحال صفته أوانتحال شخصية مالكه فيعاقب الفاعل بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة أوبغرامة لا تقل عن (200) مائتي دينار ولا تزيد على (1000) ألف دينار أوبكلتا هاتين العقوبتين.(قانون أنظمة المعلومات المؤقت، 2010)

ومن ذلك نرى ان الأثر القانوني لتسريب تلك الوثائق شديد جدا لسبب خطورة تلك الوثائق، حيث اعتبر المشروع الأردني أن ذلك الفعل فعلا غير قانوني، الأمر الذي جعل المشرع الأردني شدد العقوبة باعتبار أن ذلك العمل غير مصرح به قانونيا،

إذ أن الدخول بحد ذاته للوسائل الإلكترونية بقصد غير قانوني هوجريمة يعاقب عليها القانون، فإذا كانت دخول بهدف ارتكاب أي من الأفعال أوتحقيق أي من النتائج المذكورة في البند(ب) من المادة(3) على فعل الدخول غير المصرح به قانونيا نظرا لخطورة تشرين أوإفشاء أونقل تلك المعلومات.

يترتب على إفشاء أسرار الدولة عبر الوسائل الإلكترونية انواع من المسؤوليات التأديبية المدنية الجزائية.

أ) المسؤولية التأديبية: الجريمة التأديبية هي كل مخالفه مسلكية للواجبات الوظيفية التي يقترفها الشخص الموظف أوالعامل عند القيام بعمل أوالامتناع عن القيام بعمل مما يجعله يستحق العقاب التأديبي.

وتعد المسؤولية التأديبية دعامة أساسية للحماية القانونية لسريه المهنة بما قد يوقع عن جزاء تأديبي نتيجة التقصير في المحافظة على السر المهني باعتباره تصرفا من شانه الإخلال بواجبات الوظيفة والمهنة.

وبناء على ذلك فإن الموظف يتحمل الجزاء التأديبي القانوني في حال عدم المحافظة على السر المهني ولوبعد الاستقالة أوالإحالة على التقاعد وقد فرض المشرع الأردني في قانون العمل الأردني رقم 8 لسنة 1996 وتعديلاته اشد العقوبات التأديبية(قانون العمل الأردني رقم (8)، 1996) حيث يفصل العامل أوالموظف من دون إشعار في حال إفشاء الأسرار المهنية الخاصة بالعمل وإذا ما أفشى موظف أسرار العمل أوسرب وثيقة معنية عبر الوسائل الإلكترونية فانه يعاقب حسب المادة (14) و(15) و(16) من قانون الجرائم الإلكترونية(قانون الجرائم الإلكترونية رقم (27)، 2015).

ب) المسؤولية المدنية: تقوم المسؤولية المدنيـة باعتبـار أن هنـاك عقـداً قانونيـاً بـين الموظف والعمل، ومن صفات هـذا العقـد انـه صـحيحا واجـب التنفيـذ وملزمـا، ويترتب على عدم الالتزام بالعقد أضرار مادية وقانونيـة ومعنويـة تلحـق للدولـة وبالموظف الذي لم يلتزم بالعقد، وقد ينشا ذلك الإخلال بالعقـد مـن خـلال قيـام الموظف بنشر معلومات أوإفشاء أسرار أوتسريب وثائق محمية حكومية أوعامة، وقد ينشا الإخلال بذلك من الجهة الحكومية التي يعمل فيها الموظف من خـلال عدم القيام تلك الجهة بالوفاء بالالتزامات تجـاه الموظـف مـما يـؤدي بالتـالي إلى إفشاء أسرار الدولة ونشر الوثـائق عـبر الوسـائل الإلكترونيـة الأمـر الـذي يوجـب التعويض على الجهة المدنية أوالحكومية التي يعمـل بهـا الموظـف طبقـا للـمادة (288) من القانون المدني الأردني رقم 43 لسنة 1976 مـع كافـة تعديلاتـه والتـي تنص على:"لا يسال أحد عن فعل غـيره، ومـع ذلـك فللمحكمـة بنـاء عـلى طلـب المضرور إذا رأت مبررا أن تلزم بأداء الضمان المحكوم بـه عـلى مـن أوقـع الضرر"، من كانت له على من وقع منه الاضرار سلطة فعلية في رقابته وتوجيهه ولولم يكن حرا في اختياره إذا كان الفعل الضار قد صدر مـن التـابع في حـال تأديـة وظيفتـه أوبسببها، وبعد ذلك يستطيع البنك ان يرجع عـن الموظـف المسـؤول عـن الضرر الذي لحق بالآخرين"(القانون المدني الأردني رقم (43)، 1976).

وحتى تقوم المسؤولية الجزائية لابد من تحديد أركان الجريمة الإلكترونية وجريمة إفشاء أسرار ووثائق الدولة المحمية، وحتى يتوفر الركن المادي المتمثل بإفشـاء أونشر أوتسريب الوثائق المحمية عبر الوسائل الإلكترونية، واطلع الغـير عليهـا سـواء أكانـت شركـه الوسـائل شـفهية أوكتابيـه، إلى جانـب ذلـك يشـترط القـانون صـفه الجانـب وهوالمؤتمن على السر أوعلى جزء منه، وكذلك يجب توافر القصد الجرمي العـام دون

الخاص بركنيه العلم والإرادة، أي أننا أمام جريمة الكترونية عمدية، والشروع هنا غير معاقب عليه؛ لأننا بصدد جنحة ولا تقوم هذه الجريمة بمجرد الخطأ أوالإهمال، لان قانون العقوبات الأردني رقم (16) لسنة 1960 في المادة(71/أ) تنص على انه:"لا يعاقب على الشروع في الجنحة إلا في الحالات التي ينص عليها القانون صراحة"، إذ أن المادة (355) عقوبات من القانون ذاته نص بالعقاب على الشروع في هذه الجريمة.(قانون العقوبات الأردني رقم (16)، 1960).

يرى الباحث أن الآثار القانونية لنشر أوتسريب الوثائق المحمية تتمثل بفضح أسرار الدولة وأعمالها السياسية والاقتصادية الأمر الذي يوجب المسؤولية المدنية والعقدية والجزائية والتقصيرية ولذا فإن العقوبة كانت مغلظة لتلك الجريمة في حال توافر كافة أركان الجريمة.

الآثار الأمنية للجريمة الإلكترونية من خلال تسريب الوثائق الرسمية الحكومية:

يمتاز عصر العولمة بالتغيرات السريعة مما يضع تحديات على المؤسسات الحكومية في جوانب هامه كالأداة والتغير المستمر والتكيف مع البيئة غير المستقرة. الأمر الذي يوجب على المؤسسة الحكومية العمل في بيئة مفتوحة ومتغيره بسرعة وعليها التماشي مع هذا التغير، ويمكن القول أن الآثار الأمنية لتسريب الوثائق عبر الانترنت أوالوسائل الإلكترونية تتمثل في الآتي:

- التهديد باستغلال المعلومات الحساسة مما يضر بالدولة ومكانتها الدولية، حيث أن تسريب تلك المعلومات لها آثارها على المستوى الفردي وعلى المستوى المؤسسي الحكومي وعلى المستوى الوطني من خلال الإضرار بسمعة الدولة بنشر تلك الوثائق والمعلومات السرية.(**Murphy,2011 et al**,)

- التهديد المعلومات من خلال انتقاء المعلومات والوثائق السرية التي يتم تسريبها مما يضر بمكانه الدولة وسمعتها الاقتصادية والعسكرية والسياسية وتسريب وثائق ذات أهمية اقتصاديه تؤدي إلى معرفه أسرار الدولة الاقتصادية وأسرارها وعلاقاتها السياسية وتحركاتها العسكرية وأعداد الجيوش وخطط الجيوش والآليات العسكرية وأنواعها.(**Neal,2007 et el**,)

- التهديد بتدمير المعلومات الخاصة بالدولة من خلال تدمير مكونات البناء المعلوماتي التحتي الحساس، ولهذا نتائج وآثار أمنية على الاقتصاد والأمن الوطني من خلال نشر فيروسات معينه لتلك المعلومات.(**Rees,1998**)

- التهديد عن بعد لا يتطلب التهديد الأمنية الوجود الطبيعي للجناة وإنما يمكن التخطيط والتنظيم عن بعد، حيث ان التسريب تلك الوثائق لا يتطلب أكثر من الضغط على زر في اي وسيله الكترونية فتصبح تلك الوثيقة عابره للحدود الوطنية، مما يضر بالتالي بالأمن الوطني مثل وثائق ويكيليكس أووثائق باندورا. (**Rees,1998**)

الخفاء: ما يشكل تهديدا للدولة أن التهديدات الأمنية ونشر الوثائق المحمية للدولة يتم بسهوله إخفاء الفاعلين وسهولة التنفيذ وانخفاض التكاليف مما قد يشكل عبئا على الدولة. (**Rosenau,1997**)

تهديد مبني على المعلومات الحساسة والتي تشمل الاتصالات والبنوك المال، والطاقة الكهربائية وتوزيع الوقود والغاز، والتخزين ومصادر المياه والمواصلات وكافة الخدمات الحكومية ومواقع المؤسسات الحكومية وأعمالها ومكوناتها. (**Rosenau ,1997**)

الآثار الاجتماعية للجريمة الإلكترونية من خلال تسريب الوثائق الرسمية الحكومية

إن الآثار الاجتماعية التي تتمثل بتسريب الوثائق المحمية للدولة تاتي من خلال الأوجه الآتية:

- الشعور بالظلم والتهميش وخاصة لبعض الموظفين، وخاصة ممن لديه خلافات خاصة مع المؤسسة التي يعمل فيها أومع مديريه المباشر، الأمر الذي يؤدي وبشكل متعمد بتسريب وثائق حكومية على درجه عاليه أومتوسطه من السرية كرد فعل وانتقام علي ما يشعر به الموظف من مظلومية وعدم اعتبار.(البدانية، 2003)

- تصبح الوثائق وتسريبها هدفا اجتماعيا سهلا لكل من تسول له نفسه تسريب وثائق الدولة والإضرار بمكانتها الشعبية والوطنية والدولية، ذلك لان الحصول على المعلومات وإفشائها وتسريب الوثائق أصبح سهلا في هذه الأيام بسبب تنوع أدوات التكنولوجيا وصعوبة معرفه الفاعل مما يضر بسمعه الدولة.(سليم، 1997)

- أصبح الحصول على المعلومات بالطرق المقبولة وغير المقبولة اجتماعيا عمليه هامه نجم عنها التفكير بحمايتها خاصة إذا كانت تلك المعلومات والوثائق ذات قيمه عاليه.(**Neal,2007**)

- تعطيل البناء التحتي للمعلومات الحساسة حيث أن ذلك الأمر قد يضر بسمعه الدولة اجتماعيا، ويعوق الدولة على أداء واجباتها تجاه شعبها، وقد يؤدي إلى الفوضى الاجتماعية في حال نشر المعلومات على المستوى المحلي والدولي، الأمر الذي يستدعي اهتمام الدولة بحماية وثائقها السرية، ووجود الخطط البديلة وبحث البدائل الدفاعية اللازمة وقت الحروب، حيث ان الحروب الآن أصبحت حرب وثائق ومعلومات جيوشها الدخلاء والقراصنة والهواة والجواسيس والعملاء.(الجحني، 1398هـ)

مراجع الفصل الرابع

1. إبراهيم، خالد ممدوح(2009)، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، مصر، ط1.
2. البداينة، ذياب(2010)، الأمن الوطني في عصر العولمة، مطبعه السفر، عمان، الأردن.
3. البداينة، ذياب(2003)، إبراز الأمني في عصر المعلومات، بحث مقدم إلى الندوة العلمية(العمل إبرازي الأمني: المشكلات والحلول)، جامعه مؤتة، الكرك، الأردن، بالتعاون مع أكاديمية نايف للعلوم الأمنية، الرياض، من4-6/6/ 2003، .
4. البناء، حسين(2011)، ظاهره تسريب الوثائق الرسمية دار النهظة المصرية، القاهرة، مصر.
5. تمام، أحمد (2009). الحماية الجنائية للحاسب الآلي، دار النهضة العربية، القاهرة.
6. الجبور، محمد(2012)، الوسيط في قانون العقوبات (القسم العام)، دار وائل، عمان، الأردن، ط1.
7. الجحني، علي فايز(1398هـ)، دور إبراز الأمني في استتباب الأمن ومكافحه الجريمة، رسالة ماجستير غير منشورة، جامعة الإمام محمد بن سعود، الرياض، السعودية.
8. الجريدة الرسمية المنشور على الصفحة 4467، عدد رقم 4510، تاريخ 2000/10/8م.

9. الجنيهي، منير محمد، والجنيهي، ممـدوح محمـد (2015). بروتوكـولات وقـوانين الإنترنت، دار الفكر الجامعي، الإسكندرية، ط1.

10. حجازي، عبد الفتاح بيومي(2007)، التزوير في جـرائم الكمبيـوتر والانترنـت، دار الكتب القانونية، القاهرة، مصر.

11. حسني، محمود نجيـب (2011). النظريـة العامـة للقصـد الجنـائي، دار النهضـة العربية، ط2.

12. الحسيني، محمـد (2013). مقـال بعنـوان: "مختصـون يطـالبون بتشريـع خـاص للجـرائم الإلكترونيـة في الكويـت، منشـور في محليـات جريـدة "هنـا الكويـت" الصادرة في 12 فبراير.

13. الخوالدة، محمـد، سـليمان، جريمـة الوصـول غـير المشروعـة إلى موقـع الكـتروني اونظام معلومات وفق التشريع الأردني، دراسة مقارنة، دار الثقافة، عمان الأردن، ط1، 2012.

14. الدسوقي، محمد (2003). الحماية الجنائية السرية المعلومات، دار الفكر العربي، القاهرة، ط1.

15. رمضان، مدحت(2004)، الحماية الجنائية لموقع الإنترنت ومحتوياته، مقدمـة إلى ندوة التجارة الإلكترونية المنعقدة في المعهد العالي للعلوم القانونية والقضـائية - دبي، الإمارات العربية المتحدة 10-11مايو.

16. الرواشـدة، سـامي، والهياجنـة، أحمـد (2009). مكافحـة الجريمـة المعلوماتيـة بالتجريم والعقاب، المجلة الأردنية في القانون والعلوم السياسية، جامعة مؤتـة - الأردن، المجلد (1)، العدد (3) ص 128 وما بعدها.

17. الرومـي، محمـد أمـين (2013). جـرائم الكمبيـوتر والإنترنـت، دار المطبوعـات الجامعية، الإسكندرية.
18. الزيدي، وليـد (2009). القرصـنة عـلى الإنترنـت والحاسـوب، دار أسـامة للـنشر، عمان، ط3.
19. سلامة، محمد عبد اللــه(2017)، موسـوعة جـرائم المعلومـات، المكتـب العـربي الحديث، الإسكندرية، مصر.
20. سلطان، أنور(2011)، مصـادر الالتـزام في القـانون المـدني الأردني، دراسـة مقارنـة بالفقه الإسلامي، منشورات الجامعة الأردنية، عمان، ط1.
21. سليم، طارق عبد الوهاب، الجرائم المرتكبة بواسـطة الانترنـت وسـبل مكافحهـا، بحث منشور، مجلس وزراء الداخلية العرب، تونس، 7-9 تموز/ يوليو1997.
22. الشوا، سامي(2011)، ثورة المعلومـات وانعكاسـاتها عـلى قـانون العقوبـات، دار النهضة العربية، القاهرة، مصر.
23. عاشي، سميرة (2011). ماهية الجريمة المعلوماتية، بحث منشور في مجلة المنتدى القانوني، ع(7)، جامعة محمد خيضر بسكرة، الجزائر.
24. عبـد اللــــه، عبـد اللـــه عبـد الكـريم(2011)، جـرائم المعلومـات والانترنـت، منشروات، الحلبي الحقوقية، بيروت، لبنان، ط1.
25. عرب، يونس(2002)، إيجاز في المفهـوم والنطـاق والخصـائص والصـور والقواعـد الإجرائية للملاحقة والإثبات، مقدمة إلى مؤتمر الأمن العربي 2002 - تنظيم المركز العـربي للدراسـات والبحـوث الجنائيـة - أبـوظبي، الإمـارات العربيـة المتحـدة، 2002/2/12م.

26. قاسم، محمد عبد اللـه (2010). الحماية الجنائية للمعلومات الإلكترونيـة، دار الكتب القانونية، مصر، ط1.
27. قانون أصول المحاكمات المدنية رقم (24)، لسنة 1988، لسنة 2021 وتعديلاته.
28. قانون البيانات الأردني رقم (30)، لعام 1952.
29. قانون الجرائم الإلكترونية الأردني رقم (27) لسنة 2015.
30. قانون العقوبات الأردني، رقم (54)، لسنة 2001.
31. قانون العقوبات الأردني رقم (16) لسنة 1960، وتعديلاته لعام 2020.
32. قانون العقوبات الفرنسي لعام2020.
33. قانون العمل الأردني رقم (8) لسنة 1996.
34. القانون المدني الأردني رقم (43) لسنة 1976 مع كافه تعديلاتها.
35. قانون المعاملات الإلكترونية المؤقت رقم (6) لسنة 2013.
36. قانون أنظمة المعلومات المؤقت لسنة 2010.
37. قانون جرائم أنظمة المعلومات الأردني رقم(30) السنة 2010م.
38. قانون حماية أسرار ووثائق الدولة رقم (50) لسنة 1971، وتعديلاته.
39. قايد، أسامة عبد اللـه، الحماية الجنائية لحق المؤلف، دراسة مقارنة، دار النهضة العربية، الطبعة الأولى، القاهرة، جمهورية مصر العربية، 1991.
40. قرار محكمة التمييز - حقوق - رقم 74/45 والمنشور على الصفحة 1049 من مجلة نقابة المحامين لسنة 1974.
41. القضاة، مفلح عواد، أصول المحاكمات المدنية والتنظيم القضائي، مكتبة دار الثقافة للنشر والتوزيع، الطبعة الثالثة، عمان، الأردن، 1998.

42. لطفي، محمد حسام محمود، حقوق المؤلف في ضوء آراء الفقه وأحكام القضاء - دراسة تحليلية للقانون المصري، القاهرة، مصر، 1999 - 2000.
43. المجلس الأوروبي، مشروع اتفاقية جرائم الحاسوب، بروكسل، 27/ نيسان/ ابريل/ 2004.
44. الملـط، أحمـد خليفـة (2006). الجـرائم المعلوماتيـة، دار الفكـر الجـامعي، الإسكندرية، ط2، ص167 وما بعدها.
45. المنشاوي، محمد عبد اللـه، جرائم الإنترنت من منظـور شرعـي وقـانوني، رسـالة ماجستير، منشورة بتـاريخ 2005/5/15م عـلى الموقـع الإلكـتروني: http://www.minshawi.com/old/internetcrim-in%20the%20law.htm، .
46. منصور، امجد، المسـؤولية عـن الأضرار الناجمـة عـن الجـمادات، الـدار العلميـة الدولية، ودار الثقافة للنشر، عمان الأردن، 2012.
47. موسى، مصطفى محمد (2010). دليل التحري عبر شـبكة الإنترنـت، دار الكتـب القانونية، مصر.

المراجع الأجنبية:

1. **Murphy , Jhon, F, Computer Network Attacks By Terrorists : Some Legal Dimension, 2011, Oxford university press, oxford , London , p. 11-12.**
2. **Neal, M. Jim, L , Linaly, GH. Alexandru, catana, Doian, catana, Acomparison of leadership profotypes of Arab and European females, International Journal of cross calture management, combridge university press, Cambridge, 2007, p.36-37.**

3. **Rees, A. Crime in the information Age: prevention and Investigetion crime against Business, convened by the Australian Institste of criminology, melboctrne, 1998, p. 56-57.**
4. **Rosenau, J. N . Along the Domestic- foreign frontier exoloring Governance in a Turblent world. cambrigde university press, Cambridge, 1997, 22-23.**
5. **Usdoj(2017), The Electronic frontier:the challenge of unlawful conduct involving the use of the Internet, A Report of the President's Working Group on Unlawful Conduct on the Internet,**

   http://www.usdoj.gov/criminal/cybercrime/unlawful.htm
6. **United States V.Girard,601 F.2d 69 2d Cir 1979. .Rashmark, Crimallawand The Internet,** Http://Cla.Org/Ruhbook/ Chp11.Htm
7. **http:www.cybercrime.gov/coepress.htm**